GALOISTHEORIE

Dr.F.D.Veldkamp.

Mathematisch Instituut
Rijksuniversiteit Utrecht
1967 .

GALOISTHEORIE

Dr.F.D.Veldkamp.

Mathematisch Instituut
Rijksuniversiteit Utrecht
1967 .

In dit dictaat staan aan het eind van de meeste paragrafen opgaven die kunnen dienen ter oefening van de bestudeerde stof. Sommige daarvan zijn voorzien van een * ; deze zijn nogal moeilijk en kunnen zonder bezwaar overgeslagen worden. Aan het eind van het dictaat staat een kleine litteratuurlijst. Raadpleging van een aantal van de daarin genoemde werken is ten zeerste aan te bevelen als afwisseling bij en aanvulling op het lezen van dit dictaat.

Hoofdstuk I. Inleiding.

1. Onder een ordening op een verzameling V verstaan we een relatie $\leq$ tussen elementen van V met de volgende eigenschappen:
   1) $a \leq b$ en $b \leq a$ dan en slechts dan als $a = b$;
   2) als $a \leq b$ en $b \leq c$, dan $a \leq c$.

   V heet dan geordend. V heet totaal geordend, als voor elk tweetal elementen $a, b \in V$ geldt: $a \leq b$ of $b \leq a$. De relaties $<, \geq, >$ worden op voor de hand liggende manier ingevoerd.
   Is $W \subseteq V$, dan heet a een bovengrens van W in V, als $a \geq x$ voor alle $x \in W$. $b \in V$ heet een maximaal element van V, als uit $x \geq b$ volgt $x = b$.

(1.1) Lemma van Zorn. Is V een niet lege geordende verzameling zodat iedere totaal geordende deelverzameling een bovengrens heeft in V, dan bevat V een maximaal element.

We zullen hier geen bewijs geven voor dit lemma; zie bijvoorbeeld het dictaat Algebra van Prof.Dr.H.Freudenthal.

2. Onder een ring zullen we in dit dictaat steeds verstaan een commutatieve ring met eenheidselement, tenzij uitdrukkelijk anders vermeld wordt.
   Het eenheidselement noteren we meestal met 1.
   Een ideaal I in een ring R, $I \neq R$, heet maximaal, als voor elk ideaal J in R, $J \neq R$, uit $J \supseteq I$ volgt: $J = I$.

(2.1) Stelling. Zij I een ideaal in een ring R. I is maximaal dan en slechts dan als R/I een lichaam is.
Bewijs. Zij φ het kanonieke homomorfisme van R op R/I, d.w.z. $\varphi(x) = x + I$. Neem $\varphi(x) \neq 0$ in R/I.
We zoeken een y zodat $\varphi(x)\ \varphi(y) = \varphi(1)$, d.w.z. $xy + i = 1$ voor een $i \in I$. Bekijk het ideaal $xR + I$. Dit bevat 1 voor elke $x \notin I$ dan en slechts dan als I een maximaal ideaal is.

(2.2) Stelling. Elk ideaal I in $R, I \neq R$, is bevat in een maximaal ideaal.
Bewijs. Orden de verzameling van alle idealen $\neq R$, die I bevatten, door inclusie. Met het lemma van Zorn is dan het gevraagde maximale ideaal te vinden.

We beschouwen nu een ring R <u>zonder nuldelers</u>. $a \in R$ heet een <u>eenheid</u>, als er een $a^{-1} \in R$ is met $a a^{-1} = 1$. Is $R = \mathbb{Z}$, de ring van de gehele getallen, dan zijn ± 1 de enige eenheden. In de polynoomring $K[X]$ over een lichaam K zijn de constante veeltermen $\neq 0$ door enige eenheden.
$p \in R$ heet een <u>priemelement</u> als uit $p = ab$ volgt dat a of b een eenheid is en als p zelf geen eenheid is. In $\mathbb{Z}$ zijn de getallen $\pm p$, p een priemgetal, de priemelementen. In $K[X]$ zijn de irreducibele niet constante polynomen de priemelementen. Is p priem en a een eenheid, dan is pa priem.

R heet een <u>ontbindingsring</u> als geldt:
a) iedere $x \in R$, $x \neq 0$, is te schrijven als $a = p_1 p_2 \cdots p_r$, met $p_1, \ldots, p_r$ priemelementen;
b) geldt voor priemelementen $p_1, \ldots, p_r$, $q_1, \ldots, q_s$: $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, dan is $r = s$ en is er een permutatie σ van de getallen $1, \ldots, r$ zodat voor elke i : $p_i = e_i q_{\sigma(i)}$, e_i een eenheid.
Voorbeelden van ontbindings ringen zijn $\mathbb{Z}$ en $K[X]$.
In een ontbindingsring bestaan de grootste gemene deler (g.g.d.) en het kleinste gemene veelvoud (k.g.v.) van een aantal elementen; deze zijn op een eenheid na bepaald. In een ontbindingsring geldt: is p priem, p/ab, dan p/a of p/b.

Voor $x_1, \ldots, x_n \in R$ noteren we met $\text{ggd}(x_1, \ldots, x_r)$ de g.g.d. van $x_1, \ldots, x_r$, met $(x_1, \ldots, x_r)$ het ideaal voortgebracht door $x_1, \ldots, x_r$. Een ideaal (x), $x \in R$, heet <u>hoofdideaal</u>. Is ieder ideaal in R een hoofdideaal, dan noemen we R een <u>hoofdideaalring</u>. Men kan bewijzen, dat iedere hoofdideaalring een ontbindingsring is; zie. b.v. Jacobson, vol.I, p.122 (zie litteratuurlijst achter in dit dictaat).

(2.3) <u>Stelling</u>.
Zij R een hoofdideaalring. Zij $d = \text{ggd}(x,y)$. Dan is $(x,y) = (d)$.
<u>Bewijs.</u> Stel $(x,y) = (d)$. Dan $x \in (d)$, dus $d | x$; evenzo $d | y$.
Stel anderzijds $f | x$ en $f | y$. $d \in (x,y)$, dus $d = ax + by$. Dus $f | d$.
Dus $d = \text{ggd}(x,y)$.

(2.4) <u>Stelling</u>. Stel K en L zijn lichamen, $K \subset L$. Voor f, g in $K[X]$ is dan $\text{ggd}(f,g)$ in $K[X]$ hetzelfde als $\text{ggd}(f,g)$ in $L[X]$.
<u>Bewijs.</u> Dit is een onmiddellijk gevolg van de vorige stelling.

(2.5) Stelling. Is R een ontbindingsring, dan ook $R[X]$.
Bewijs. Neem $f \in R[X]$. $f = a_0 + a_1X + \ldots + a_n X^n$, met $a_i = R$. $\delta(f) = ggd(a_0, a_1, \ldots, a_n)$ noemen we de inhoud van f; deze is bepaald op een eenheid na.
We tonen aan dat $\delta(fg) = \delta(f) \cdot \delta(g)$. Stel $f = \delta(f)f_1$, $g = \delta(g)g_1$. f_1 en g_1 hebben dus inhoud 1. $fg = \delta(f)\,\delta(g)\,f_1g_1$. We zijn klaar als we kunnen bewijzen dat f_1g_1 inhoud 1 heeft. Zij p een priemfactor van $\delta(f_1g_1)$; alle coëfficienten van fg zijn dus deelbaar door p. Zij f' de veelterm die uit f_1 ontstaat door alle termen weg te laten waarvan de coëfficienten deelbaar zijn door p, en g' de veelterm die zo uit g_1 ontstaat. Dan geldt ook voor f'g' dat alle coëfficienten deelbaar zijn door p. Anderzijds is p noch een deler van de hoogste coëfficient van f' noch van die van g', dus ook niet van de hoogste coëfficient van f'g'. Tegenspraak. Derhalve is $\delta(f_1g_1) = 1$.
Neem $f \in R[X]$. Dan $f = \delta(f)g$, $\delta(g) = 1$. We laten zien dat g in priemfactoren ontbonden kan worden, en wel op één manier - afgezien van de volgorde en van eenheden.
Zij K het quotientenlichaam van R. In $K[X]$ is g op één manier te ontbinden in irreducibele polynomen - op volgorde en eenheden na. Dus $g = p_1 \ldots p_r$, p_i irreducibel in $K[X]$.
We schrijven $p_i = \frac{\mu_i}{\lambda_i} p_i'$, $p_i' \in R[X]$, $\delta(p_i') = 1$, λ_i, $\mu_i \in R$, $ggd(\lambda_i, \mu_i) = 1$. Dan is

$$\lambda_1 \ldots \lambda_r\, g = \mu_1 \ldots \mu_r\, p_1' \ldots p_r' .$$

Neem de inhoud van beide leden van deze vergelijking, dan krijgt men

$$\lambda_1 \ldots \lambda_r = \mu_1 \ldots \mu_r .$$

Dus

$$g = p_1' \ldots p_r' .$$

Ga na dat de p_i' priemelementen in $R[X]$ zijn. De eenduidigheid van de ontbinding van g in $R[X]$ volgt uit die in $K[X]$.

Merk op dat voor $g \in R[X]$ de ontbinding in irreducibele factoren in $R[X]$ tevens een ontbinding in irreducibele factoren in $K[X]$ is.

(2.6) Stelling. Zij R een hoofdidealring die tevens ontbindingsring is (zie opmerking vóór (2.3)). Dan is (a) een maximaal ideaal in R dan en slechts dan als a een priemelement in R is.

Bewijs. Stel (a) maximaal. Is $a = bc$, dan is $(a) \subseteq (b)$. Dus $(b) = R$ of $(b) = (a)$. In het eerste geval is $1 \in (b)$, dus b is een eenheid. In het tweede geval $b = ea$, e een eenheid. Omdat R geen nuldelers bevat, is $c = e^{-1}$, d.w.z. c een eenheid. Dus a is priem.
Zij omgekeerd a een priemelement. Stel $(a) \subseteq (b)$. Dan is er een c zodat $a = bc$. Dus b of c is een eenheid, d.w.z. $(b) = R$ of $(b) = (a)$. Dus (a) is een maximaal ideaal.

Opgaven.
1. Beschouw de polynoomring $K[X,Y]$ over een lichaam K. Bewijs dat (X,Y) geen hoofdideaal is.

2. $\mathbb{F}_5$ is het priemlichaam van karakteristiek 5, d.w.z. $\mathbb{F}_5 = \mathbb{Z}/(5)$. Ontbind het volgende polynoom in $\mathbb{F}_5[X]$ in irreducibele factoren.

$$X^4 + 3X^3 + 3X^2 + X + 2.$$

3. Zij K een lichaam, $f \in K[X]$ een veelterm van de graad 2 of 3. Bewijs: f is irreducibel dan en slechts dan als f geen wortels heeft in K, d.w.z. als er geen $x \in K$ bestaat zodat $f(x) = 0$. Is dit ook nog waar als de graad van $f > 3$ is?

4. Alle polynoomringen $K[X_1, \ldots, X_n]$ over een lichaam K zijn ontbindingsringen. Bewijs dit.

3. Zij R een ring (als steeds commutatief met 1). M heet een R-moduul als M een optelgroep is waarin bovendien een scalaire vermenigvuldiging is gedefinieerd: voor $\lambda \in R$ en $x \in M$ is er precies één $\lambda x \in M$, zodanig dat aan de volgende eisen is voldaan:
1) $1x = x$ voor alle $x \in M$;
2) $(\lambda + \mu)x = \lambda x + \mu x$ voor $\lambda, \mu \in R$, $x \in M$;
3) $(\lambda\mu)x = \lambda(\mu x)$ voor $\lambda, \mu \in R$, $x \in M$
4) $\lambda(x+y) = \lambda x + \lambda y$ voor $\lambda \in R$, $x, y \in M$.

Is R een lichaam, dan spreekt men ook van een R-lineaire ruimte of vectorruimte. Deelmodulen en factormodulen worden op de gebruikelijke wijze gedefinieerd. Zijn M en N R-modulen, dan heet een afbeelding $f: M \to N$ een R-homomorfisme of R-lineaire afbeelding, als
1) $f(x+y) = f(x) + f(y)$ voor $x, y \in M$;
2) $f(\lambda x) = \lambda f(x)$ voor $\lambda \in R$, $x \in M$.

Ga na dat $f(0) = 0$, $f(-x) = -f(x)$. Een 1-1 R-homomorfisme op heet een R-isomorfisme; een R-isomorfisme heeft een R-lineaire inverse.

Zijn M, N en P R-modulen, dan is een R-bilineaire afbeelding $f : M \times N \to P$ een afbeelding waarvoor geldt

$$f(x_1+x_2, y) = f(x_1, y) + f(x_2, y) \quad ,$$
$$f(x, y_1+y_2) = f(x, y_1) + f(x, y_2) \quad ,$$
$$f(\lambda x, y) = f(x, \lambda y) = \lambda f(x, y) \quad ,$$

voor alle $\lambda \in R$, $x, x_i \in M$, $y, y_i \in N$.

(3.1) Stelling. Bij twee R-modulen M en N is er een R-moduul T met de volgende eigenschappen :

1) Er is een R-bilineaire afbeelding $f : M \times N \to T$;

2) Is P een R-moduul en g een R-bilineaire afbeelding : $M \times N \to P$, dan is er precies één R-lineaire afbeelding $h : T \to P$ zodat $g = h \circ f$, d.w.z. het volgende diagram is commutatief:

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & P \\ {\scriptstyle f}\downarrow & \nearrow {\scriptstyle h} & \\ T & & \end{array}$$

T is op isomorfisme na bepaald door de eisen 1) en 2). T heet het tensorproduct van M en N; notatie: $T = M \otimes_R N$ (of $M \otimes N$, als geen verwarring mogelijk is). Voor $f(x,y)$ schrijven we ook $x \otimes y$.

$(x_1+x_2) \otimes y = x_1 \otimes y + x_2 \otimes y$, $x \otimes (y_1+y_2) = x \otimes y_1 + x \otimes y_2$,

$(\lambda x) \otimes y = x \otimes (\lambda y) = \lambda (x \otimes y)$.

Iedere $z \in M \otimes N$ is te schrijven als $z = \sum_{i=1}^{n} x_i \otimes y_i$, $x_i \in M$, $y_i \in N$.

Bewijs. (i) Existentie van T. Neem het vrije moduul V voortgebracht door $M \times N$; elementen van V zijn de eindige sommen $\sum \lambda_i (x_i, y_i)$ met $\lambda_i \in R$, $x_i \in M$, $y_i \in N$, optelling en scalaire vermenigvuldiging gebeuren coördinaatsgewijs.

In V beschouwen we het deelmoduul I voortgebracht door de elementen

$$(x_1+x_2, y) - (x_1, y) - (x_2, y) \quad ,$$
$$(x, y_1+y_2) - (x, y_1) - (x, y_2) \quad ,$$
$$(\lambda x, y) - \lambda (x, y) \quad ,$$
$$(x, \lambda y) - \lambda (x, y) \quad ,$$
$$\lambda \in R\ ,\ x, x_i \in M,\ y, y_i \in N \ .$$

We nemen nu $T = V/I$. $f : M \times N \to T$ definiëren we door

$f(x,y) = (x,y) + I$; ga na dat f R-bilineair is.

Zij nu P een R-moduul en g R-bilineair: $M \times N \to P$. g definieert $\bar{g} : V \to P$ door

$$\bar{g}\,(\Sigma\, \lambda_i (x_i, y_i)) = \Sigma\, \lambda_i\, g(x_i, y_i)\ .$$

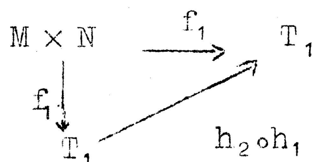
$\bar{g}$ is een R-lineaire afbeelding. Door $\bar{g}$ te laten werken op de voortbrengenden van I ziet men zonder veel moeite in dat $\bar{g}(I) = 0$. Dus is er een R-lineaire afbeelding $h : T \to P$ zodat $h\,(z \bmod I) = \bar{g}(z)$ voor $z \in V$. Kennelijk is $h \circ f = g$. h is hierdoor vastgelegd, want $h \circ f = g$ impliceert $h(f(x,y)) = g(x,y)$ en T wordt voortgebracht als R-moduul door de elementen $f(x,y)$.

(ii) Eenduidigheid van T. Stel T_1 en T_2 voldoen beide aan 1) en 2), met bilineaire afbeeldingen $f_i : M \times N \to T_i$.

Bij $f_2 : M \times N \to T_2$ is er dan een $h_1 : T_1 \to T_2$, zodat $h_1 \circ f_1 = f_2$.

Evenzo is er een $h_2 : T_2 \to T_1$, zodat $h_2 \circ f_2 = f_1$.

Beschouw nu het volgende commutatieve diagram :



Er is precies één afbeelding h zodat $h \circ f_1 = f_1$, n.l. de identiteit van T_1. Dus is $h_2 \circ h_1$ de identiteit. Evenzo is $h_1 \circ h_2$ de identiteit, dus $h_2 = h_1^{-1}$. h_1 is derhalve een isomorfisme : $T_1 \to T_2$.

(iii) Uit de constructie onder (i) volgt dat iedere $z \in M \otimes N$ te schrijven is als $z = \Sigma\, \lambda_i (x_i \otimes y_i)$. Maar dan is ook $z = \Sigma(\lambda_i x_i) \otimes y_i$.

Let wel, de schrijfwijze $z = \Sigma\, x_i \otimes y_i$ is allerminst eenduidig.

(3.2) Stelling. M, N, M_1 , N_1 R-modulen, f en g R-homomorfismen, $f : M \to M_1$, $g : N \to N_1$. Dan is er precies één R-homomorfisme $f \otimes g : M \otimes N \to M_1 \otimes N_1$, zodat

$$f \otimes g\ (x \otimes y) = f(x) \otimes g(y).$$

Bewijs. We definiëren een bilineaire afbeelding

$$h : M \times N \to M_1 \otimes N_1$$

door: $\quad h(x,y) = f(x) \otimes g(y)$.

Er is precies één lineaire afbeelding

$$k : M \otimes N \to M_1 \otimes N_1 ,$$

zodat $\quad k(x \otimes y) = h(x,y)$, volgens (3.1).

Neem $\quad f \otimes g = k$.

M noemen we een <u>directe som</u> van deelmodulen M_α , notatie:

$$M = \oplus M_\alpha \ ,$$

als iedere $x \in M$ op precies één manier te schrijven is als

$$x = \Sigma\, x_\alpha \ , \ x_\alpha \in M_\alpha \ ,$$

met slechts eindig veel $x_\alpha \neq 0$. In geval van een eindige directe som schrijven we ook wel

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_n \ .$$

Is M_1 een deelmoduul van M, dan definieert de injectie $i = M_1 \to M$, (d.w.z. de afbeelding met $i(x) = x$ voor $x \in M_1$) een R-homomorfisme $i \otimes 1 : M_1 \otimes N \to M \otimes N$. Helaas is $i \otimes 1$ niet altijd 1-1, d.w.z. we kunnen $M_1 \otimes N$ niet op natuurlijke wijze identificeren met een deelmoduul van M. (zie opgave 2 aan het einde van deze paragraaf).

Is M een directe som $M = M_1 \oplus M_2$, dan is $i \otimes 1$ wel 1-1; algemener geldt:

(3.3) <u>Stelling</u>. Zijn $M = \underset{\alpha}{\oplus} M_\alpha$ en N R-modulen, dan is

$$M \otimes N \cong \oplus (M_\alpha \otimes N).$$

<u>Bewijs</u>. $\pi_\alpha = M \to M_\alpha$ definiëren we als volgt: is

$$x = \sum_\gamma x_\gamma,\ x_\gamma \in M_\gamma,$$

dan $\qquad \pi_\alpha\ x = x_\alpha.$

De afbeelding $f = M \times N \to \oplus (M_\alpha \otimes N)$ met

$$f(x,y) = \oplus (\pi_\alpha x) \otimes y$$

is bilineair.

Zij verder $g: M \times N \to P$ bilineair. Beschouw de restrictie g_α van g tot $M_\alpha \times N$; g_α is bilineair, dus definieert een lineaire afbeelding

$$h_\alpha : M_\alpha \otimes N \to P$$

zodat $\qquad h_\alpha(x_\alpha \otimes y) = g_\alpha(x_\alpha, y) = g(x_\alpha, y).$

Definieer $\qquad h : \oplus (M_\alpha \otimes N) \to P$ door

$$h(\sum_\alpha z_\alpha) = \sum_\alpha h_\alpha(z_\alpha) \quad \text{voor } z_\alpha \in M_\alpha \otimes N.$$

h is lineair en $h \circ f = g$. h is eenduidig bepaald door deze eis. $\oplus(M_\alpha \otimes N)$ voldoet dus aan de eisen voor het tensorproduct, d.w.z. $M \otimes N \cong \oplus (M_\alpha \otimes N)$.

(3.4) <u>Gevolg</u>. Zijn $M = \oplus M_\alpha$ en $N = \oplus N_\beta$ R-modulen, dan is

$$M \otimes N \cong \underset{\alpha,\beta}{\oplus} (M_\alpha \otimes N_\beta).$$

De verzameling $\{x_\alpha\}_\alpha, x_\alpha \in M$, noemen we een <u>basis</u> van M, als ieder element van M op precies één manier geschreven kan worden als

een eindige som

$$x = \sum_\alpha \lambda_\alpha x_\alpha \ , \quad \lambda_\alpha \in R.$$

Equivalent hiermee is:

(i) $\{x_\alpha\}$ spant M op, d.w.z. iedere x is te schrijven als $x = \sum \lambda_\alpha x_\alpha$.

(ii) De x_α zijn lineair onafhankelijk over R, d.w.z. uit $\sum \lambda_\alpha x_\alpha = 0$ (eindige som) volgt: $\lambda_\alpha = 0$ voor alle α.

Heeft M een basis $\{x_\alpha\}$, dan is $M \cong \bigoplus_\alpha Rx_\alpha$, $Rx_\alpha \cong R$. Uit (3.4) volgt dus

(3.5) Stelling. Is $\{x_\alpha\}_\alpha$ een basis van M , $\{y_\beta\}_\beta$ een basis van N, dan is $\{x_\alpha \otimes y_\beta\}_{\alpha,\beta}$ een basis van $M \otimes N$.

Niet ieder moduul heeft een basis. Vectorruimten over een lichaam hebben dit wel. Daarvoor volgt dus speciaal uit (3.5):

(3.6) Gevolg. Zijn V en W vectorruimten over een lichaam k, dan is $\dim (V \otimes_k W) = \dim V. \dim W$.

(3.7) Stelling. Zijn M en N R-modulen, dan is $M \otimes N \cong N \otimes M$.

Bewijs. $f: M \times N \to N \otimes M$ met

$$f(x,y) = y \otimes x$$

is bilineair. Is $g: M \times N \to P$ bilineair, dan $g': N \times M \to P$ met

$$g'(y,x) = g(x,y)$$

ook bilineair. Er is dus precies één $h: N \otimes M \to P$ met

$$h(y \otimes x) = g'(y,x) = g(x,y) \quad ,$$

d.w.z. $g = h \circ f$. Dus is $M \otimes N \cong N \otimes M$.

Opmerking. Bovenstaande stelling houdt niet in, dat in $M \otimes M$ geldt: $x \otimes y = y \otimes x$ voor alle x en $y \in M$. Neem bijvoorbeeld het geval dat M een basis $\{x_\alpha\}_\alpha$ heeft. $\{x_\alpha \otimes x_\beta\}_{\alpha,\beta}$ is dan een basis van $M \otimes M$, dus voor $\alpha \neq \beta$ zijn $x_\alpha \otimes x_\beta$ en $x_\beta \otimes x_\alpha$ lineair onafhankelijk, derhalve zeker verschillend.

Zij nu I een willekeurige verzameling. Stel dat voor iedere $\alpha \in I$ een R-moduul M_α gegeven is. Onder $\prod_I M_\alpha$ verstaan we het directe product van de verzamelingen M_α; de elementen van $\prod_I M_\alpha$ noteren we als (x_α).

Zij N een R-moduul. Een afbeelding

$$f: \prod_I M_\alpha \to N$$

noemen we R-multilineair, als voor alle β geldt:

$$f((x_\alpha)) = f((y_\alpha)) + f((z_\alpha)) \text{ , als } x_\beta = y_\beta + z_\beta \text{ , } x_\alpha = y_\alpha = z_\alpha \text{ voor } \alpha \neq \beta \text{ .}$$

$$f((x_\alpha)) = \lambda f((y_\alpha)) \text{ als } x_\beta = \lambda y_\beta, \ x_\alpha = y_\alpha \text{ voor } x \neq \beta \text{ .}$$

Er geldt dan, analoog aan (3.1) :

(3.8) Stelling. Gegeven R-modulen M_α, $\alpha \in I$. Dan is er een R-moduul T met de volgende eigenschappen :

1) Er is een R-multilineaire afbeelding $f : \prod_I M_\alpha \to T$.
2) Is N een R-moduul en $g: \prod_I M_\alpha \to N$ een R-multilineaire afbeelding, dan is er precies één R-lineaire afbeelding $h: T \to N$, zodat $g = h \circ f$.

T is op isomorfie na bepaald door de eisen 1) en 2). T heet het tensorproduct van de M_α: $T = \bigotimes_{I R} M_\alpha$ of $\otimes M_\alpha$.

Voor $f((x_\alpha))$ schrijven we ook $\otimes x_\alpha$. Iedere $z \in \otimes M_\alpha$ is te schrijven als $z = \sum_i \otimes x_\alpha^{(i)}$, met $x_\alpha^{(i)} \in M_\alpha$.

Bewijs. Dit loopt in grote trekken hetzelfde als dat van (3.1). Men neemt het vrije moduul V voortgebracht door de elementen van $\prod_\alpha M_\alpha$ en beschouwt daarin het ideaal voortgebracht door de elementen

$(x_\alpha) - (y_\alpha) - (z_\alpha)$ met $x_\beta = y_\beta + z_\beta$ voor een $\beta \in I$, $x_\alpha = y_\alpha = z_\alpha$ voor $\alpha \neq \beta$,
$(x_\alpha) - \lambda(y_\alpha)$ met $x_\beta = \lambda y_\beta$ voor een $\beta \in I$, $x_\alpha = y_\alpha$ voor $\alpha \neq \beta$.
V/I is dan het gezochte R-moduul T.

(3.9) Stelling. Zijn M_1, M_2 en M_3 R-modulen, dan is $(M_1 \otimes M_2) \otimes M_3 \cong \bigotimes_{i=1}^{3} M_i \cong M_1 \otimes (M_2 \otimes M_3)$. Analoge uitspraken gelden voor n-tallen modulen $M_1, \ldots, M_n$.

Bewijs. We beschouwen alleen het geval n=3. Men moet laten zien dat bijv. $(M_1 \otimes M_2) \otimes M_3$ voldoet aan de in (3.8) gestelde eisen 1) en 2).

Ad 1) $f : (x,y,z) \to (x \otimes y) \otimes z$ is trilineair.

Ad 2) Is g multilineair van $\prod_{i=1}^{3} M_i \to N$, dan nemen voor $z \in M_3$:

$$g_z : M_1 \times M_2 \to N$$

met $$g_z(x,y) = g(x,y,z) ,$$

g_z is bilineair, dus is er een lineaire afbeelding

$$h_z : M_1 \otimes M_2 \to N$$

met $$h_z(x \otimes y) = g(x,y,z).$$

De afbeelding

$$g' : (M_1 \otimes M_2) \times M_3 \to N$$

met
$$g'\left(\sum_i x_i \otimes y_i , z\right) = \sum_i g(x_i, y_i, z)$$

is bilineair, dus is er een

$$h : (M_1 \otimes M_2) \otimes M_3 \to N$$

met
$$h((x \otimes y) \otimes z) = g(x,y,z).$$

h voldoet aan eis 2) en is kennelijk de enige die dat doet.

(3.10) Stelling. Zij M een R-moduul. Dan is $M \otimes_R R \cong M$.

Bewijs. Men moet weer bewijzen, dat M aan de eisen 1) en 2) voldoet voor het tensorproduct van M en R.

Ad 1) $f : M \times R \to M$ met

$$f(x,\lambda) = \lambda x$$

is bilineair.

Ad 2) Is $g : M \times R \to N$ bilineair, neem dan

$$h : M \to N \text{ met } h(x) = g(x,1).$$

(3.11) Stelling. Is M een R-moduul, R een deelring van S. Dan is S op te vatten als R-moduul en $M \otimes_R S$ als S-moduul.

Bewijs. Neem voor $\lambda \in R$, $x \in S$, als scalaire vermenigvuldiging in S het gewone product λx.

Voor $\lambda \in S$ is $g_\lambda : M \times S \to M \otimes_R S$ met

$$g_\lambda(x,\xi) = x \otimes \lambda\xi$$

bilineair. Dus is er een lineaire afbeelding

$$h_\lambda : M \otimes_R S \to M \otimes_R S$$

met
$$h_\lambda\left(\sum_i x_i \otimes \xi_i\right) = \sum_i x_i \otimes \lambda\xi_i .$$

Definieer scalaire vermenigvuldiging in $M \otimes S$ met $\lambda \in S$ nu door $\lambda z = h_\lambda(z)$ voor $z \in M \otimes S$.

(3.12) Stelling. Heeft het R-moduul M een basis $\{x_\alpha\}$ en is R een deelring van S, dan is $\{x_\alpha \otimes 1\}$ een S-basis van $M \otimes_R S$.

Bewijs. Dit volgt uit (3.3) en (3.10).

$$M \cong \oplus R x_\alpha \text{ met } R x_\alpha \cong R, \text{ dus}$$

$$M \otimes_R S \cong \oplus ((R x_\alpha \otimes S) = \oplus S (x_\alpha \otimes 1).$$

Verder is $S(x_\alpha \otimes_R 1) = R x_\alpha \otimes_R S \cong R \otimes_R S \cong S$.

Dit betekent dat de $x_\alpha \otimes 1$ een S-basis vormen van $M \otimes_R S$.

Zij R een ring. A heet een R-algebra als geldt:

1) A is een (niet noodzakelijk commutatieve) ring (met of zon-

der 1) ;

2) A is een R-moduul; de optelling in het moduul is dezelfde als die in de ring ;

3) $\alpha(xy) = (\alpha x)y = x(\alpha y)$ voor $\alpha \in R$, $x,y \in A$.

Een R-<u>algebrahomomorfisme</u> is een R-lineaire afbeelding, die tevens ringhomomorfisme is.

Heeft A een eenheidselement e, dan zit Re in het centrum van A. De afbeelding $i: R \to A$ met $i(\lambda) = \lambda e$

is een algebrahomomorfisme. Is bijv. R een lichaam, dan is i een isomorfisme. Men identificeert Re dan met R.

Zijn A en B R-algebra's dan vormen we het tensorproduct $A \otimes_R B$ van A en B als R-modulen. We definiëren een vermenigvuldiging in $A \otimes B$ op de volgende manier :

$$(\sum_i a_i \otimes b_i)(\sum_j a'_j \otimes b'_j) = \sum_{i,j} (a_i a'_j) \otimes (b_i b'_j) .$$

We dienen te bewijzen, dat dit goed gedefinieerd is.

Neem a en b vast in A resp. B. Dan is

$$f_{a,b} : A \times B \to A \otimes B$$

met

$$f_{a,b}(a',b') = (aa') \otimes (bb')$$

bilineair. Dus is er een lineaire afbeelding

$$g_{a,b} : A \otimes B \to A \otimes B$$

met

$$g_{a,b}(\sum_j a'_j \otimes b'_j) = \sum_j (aa'_j) \otimes (bb'_j).$$

Voor vaste $z = \sum_j a'_j \otimes b'_j \in A \otimes B$ is

$$h_z : A \times B \to A \otimes B$$

met

$$h_z(a,b) = g_{a,b}(z)$$

weer bilineair. Dus is er een lineaire afbeelding

$$k_z : A \otimes B \to A \otimes B$$

met

$$k_z(\sum_i a_i \otimes b_i) = \sum_i h_z(a_i,b_i)$$

$$= \sum_{i,j} (a_i a'_j) \otimes (b_i b'_j) ,$$

waarmee het product gedefinieerd is. Ga zelf na dat $A \otimes_R B$ met dit product een R-algebra is geworden.

Op analoge manier definiëert men voor een willekeurige collectie algebra's A_α het tensorproduct $\otimes A_\alpha$ als algebra.

Is A een R-algebra en R een deelring van S, dan kan men $A \otimes_R S$ weer als S-algebra opvatten. Ga dit zelf na.

Als toepassing van het voorgaande zullen we de volgende nuttige stelling bewijzen.

(3.13) Stelling. Zij K een lichaam, L_α, $\alpha \in I$, een collectie uitbreidingslichamen van K. Dan is er een uitbreiding L van K en een collectie isomorfismen i_α van L_α in L, zodat L wordt voortgebracht door de vereniging van $i_\alpha(L_\alpha)$.

Bewijs. We kunnen de L_α opvatten als K-algebra's. Beschouw de algebra $T = \bigotimes_{\alpha K} L_\alpha$. $j_\alpha : L_\alpha \to T$ is het K-homomorfisme dat $x \to \bigotimes_\gamma x_\gamma$ waarin $x_\alpha = x, x_\gamma = 1$ voor $\gamma \neq \alpha$. Kennelijk is $j_\alpha(1) = 1$, dus j_α is een isomorfisme.
Zij M een maximaal ideaal van T. $j_\alpha(L_\alpha) \cap M$ is een ideaal in $j_\alpha(L_\alpha)$ dat 1 niet bevat, dus $j_\alpha(L_\alpha) \cap M = 0$. $T/M = L$ is een lichaam. Zij p het kanonieke homomorfisme $T \to T/M = L$. Dan is $i_\alpha = p \circ j_\alpha$ een K-isomorfisme van L_α in L. T wordt voortgebracht door de $j_\alpha(L_\alpha)$, dus L door de $i_\alpha(L_\alpha)$.

Opgaven.

1. Zij V een K-lineaire ruimte met basis $e_1, \dots, e_p$, W één met basis $f_1, \dots, f_q$. Op $V \otimes_K W$ nemen we de basis $e_i \otimes f_j = e_{i,j}$. Zij A een lineaire afbeelding van V in zichzelf met matrix $(\alpha_{i,j})$ t.o.v. de gegeven basis, B een lineaire afbeelding van W in zichzelf met matrix $(\beta_{i,j})$. Laat zien dat $A \otimes B$ t.o.v. de basis $e_{i,j}$ voorgesteld wordt door de matrix $(\gamma_{i,j;k,l})$ met $\gamma_{i,j;k,l} = \alpha_{i,k} \beta_{j,l}$.

2. Beschouw de $\mathbb{Z}$-modulen $\mathbb{Z}$, $2\mathbb{Z}$ en $\mathbb{Z}/(2)$.
Zij i de injectie: $2\mathbb{Z} \to \mathbb{Z}$. Laat zien dat $i \otimes 1 : 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$ de nulafbeelding is en dat $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \cong \mathbb{Z}/(2)$.

3. V en W zijn lineaire ruimten over een lichaam K.
Stel $\sum_{i=1}^{n} a_i \otimes_K b_i = 0$ voor $a_i \in V$, $b_i \in W$. Bewijs dat één van de volgende uitspraken moet gelden.
(i) $a_1 = a_2 \dots = a_n = 0$.
(ii) $b_1, \dots, b_n$ zijn lineair afhankelijk.
Analoog met verwisseling van de a_i en b_i in (i) en (ii).

Hoofdstuk II. Uitbreidingen van lichamen.

4. Zij L een lichaam, K een deellichaam van L, dan heet L ook wel een uitbreiding van K. We vatten L op als lineaire ruimte over K. De dimensie van L over K noemen we de graad van de uitbreiding; notatie: $|L:K|$. We laten ook toe dat $|L:K| = \infty$.

(4.1) Stelling. Zij L een uitbreiding van K, M één van L.
Dan geldt:
(i) Is $\{x_\alpha\}$ een K-lineair onafhankelijk stelsel in L, $\{y_\alpha\}$ een L-lineair onafhankelijk stelsel in M, dan is het stelsel $\{x_\alpha y_\beta\}$ K-lineair onafhankelijk.
(ii) Is $\{x_\alpha\}$ een K-basis van L, $\{y_\beta\}$ een L-basis van M, dan is $\{x_\alpha y_\beta\}$ een K-basis van M.
(iii) $|M:K| = |M:L|\,|L:K|$.

Bewijs. (i) Stel $\sum_{\alpha,\beta} \lambda_{\alpha,\beta} x_\alpha y_\beta = 0$ met $\lambda_{\alpha,\beta} \in K$.

Dan is $\sum_\beta \left(\sum_\alpha \lambda_{\alpha,\beta} x_\alpha \right) y_\beta = 0$. Omdat de y_β L-lineair onafhankelijk zijn, is $\sum_\alpha \lambda_{\alpha,\beta} x_\alpha = 0$. voor alle β.
Dan moet $\lambda_{\alpha,\beta} = 0$ zijn voor alle α en β.
(ii) Stel $x \in M$. Dan $x = \sum_\beta \lambda_\beta y_\beta$, met $\lambda_\beta \in L$.
$\lambda_\beta = \sum_\alpha \lambda_{\alpha,\beta} x_\alpha$ met $\lambda_{\alpha,\beta} \in K$. Dus is

$x = \sum_{\alpha,\beta} \lambda_{\alpha,\beta} x_\alpha y_\beta$. Gezien (i) volgt hieruit dat de $x_\alpha y_\beta$ een K-basis van M vormen.
(iii) is een direct gevolg van (ii).

Zij L een uitbreiding van het lichaam K. Voor $x_1,\dots,x_n \in L$ verstaan we onder $K[x_1,\dots,x_n]$ de kleinste deelring van L die K en de elementen $x_1,\dots,x_n$ bevat, onder $K(x_1,\dots,x_n)$ het kleinste deellichaam van L dat K en $x_1,\dots,x_n$ bevat.
$K(x_1,\dots,x_n)$ is het quotiëntenlichaam van $K[x_1,\dots,x_n]$.
We zeggen dat $K(x_1,\dots,x_n)$ uit K verkregen is door adjunctie van $x_1,\dots,x_n$ aan K.
Is $K[X]$ een polynoomring over K, dan noemen we het quotiëntenlichaam van $K[X]$ het lichaam van rationale functies over K; notatie: $K(X)$. Elementen van $K(X)$ zijn voor te stellen door breuken $\frac{f}{g}$, met f en $g \in K[X]$, waarmee op de bekende wijze gerekend wordt.

We beschouwen nu speciaal een uitbreiding met één element $K(x)$ van K. Het ringhomomorfisme φ: $K[X] \to K(x)$ wordt gedefinieerd door:

$$\varphi(f) = f(x).$$

$\varphi(K[X]) = K[x]$. Er zijn twee gevallen mogelijk.

(i) φ is een isomorfisme. Dan is $K[x] \cong K[X]$, dus $K(x) \cong K(X)$. x heet transcendent over K.

(ii) φ heeft een kern $I \neq 0$. I is een ideaal in $K[X]$, dus $I = (f)$. f is een polynoom met minimale graad zodat $f(x) = 0$. f is op een factor $\neq 0$ uit K na bepaald. f heet een minimum-polynoom van x over K. x heet algebraïsch over K.

Stel $f = gh$. Dan $g(x)h(x) = 0$, dus $g(x) = 0$ of $h(x) = 0$. Stel bijv. $g(x) = 0$. Omdat f minimaal was zodat $f(x) = 0$, is $g = cf, c \in K$. f is dus irreducibel. Daaruit volgt dat (f) een maximaal ideaal is in $K[X]$, dus $K[X]/(f)$ is een lichaam. Dus $K[X]/(f) \cong K(x) = K[x]$. Een basis van $K[X]/(f)$ over K is: $1, X + (f), X^2 + (f), \ldots, X^{n-1} + (f)$, dus een basis van $K(x)$ over K is $1, x, x^2, \ldots, x^{n-1}$, als $n = gr(f)$, de graad van f.

Beschouw omgekeerd een irreducibele veelterm $f \in K[X]$. $K[X]/(f)$ is dan een lichaam. Neem $x = X + (f)$. Dan is $f(x) = f(X + (f)) = f(X) + (f) = (f) = 0$, dus x is een wortel van f; f is minimum-veelterm van x. We hebben dus bewezen:

(4.2) Stelling. Is x algebraïsch over K, dan is er een polynoom f met minimale graad zodat $f(x) = 0$; f is irreducibel en heet een minimumpolynoom van x. f is op een factor $\neq 0$ uit K na bepaald. Is omgekeerd f irreducibel in $K[X]$, dan is er een uitbreiding $K(x)$ van K zodat f minimumveelterm is van x. $|K(x): K| = gr(f)$, de graad van f.

Opgaven.

1. Ga na of de volgende veeltermen rationale wortels hebben.

a. $4X^3 - 2X + 1$.

b. $X^n - p$ (p priemgetal).

c. $8X^5 + 3X^2 - 17$.

[Aanwijzing. Is α rationaal, dan $\alpha = mn^{-1}$ met gehele m en n, die we onderling ondeelbaar mogen veronderstellen. Is f een polynoom met gehele coëfficiënten, beschouw dan de vergelijking $f(\alpha) = 0$. Maak hiervan een vergelijking voor gehele getallen door de noemers weg te vermenigvuldigen. Onderzoek die met

behulp van deelbaarheid van gehele getallen door priemgetallen].

2. Laat zien dat $f(X) = X^3+2X+1$ irreducibel is in $\mathbb{F}_5[X]$. Hoeveel elementen bevat $\mathbb{F}_5(x)$, als x een wortel van f is?

3. Wat is de minimumveelterm van $\sqrt{3}+1$ over $\mathbb{Q}$ (= het lichaam van de rationale getallen) ?

5. Een uitbreiding L van K heet <u>algebraïsch over K</u> als iedere $x \in L$ algebraïsch is over K; is dit niet het geval, dan heet L <u>transcendent over K</u>. L noemen we <u>eindig voortgebracht over K</u>, als er $x_1,\ldots,x_n \in L$ bestaan, zodat $L = K(x_1,\ldots,x_n)$.

(5.1) <u>Stelling</u>. Zij L een uitbreiding van K met $|L:K|$ eindig. Dan is L eindig voortgebracht en algebraïsch over K.
<u>Bewijs.</u> Zij $|L:K| = n$. Is $a_1,\ldots,a_n$ een basis van L over K, dan is zeker $L = K(a_1,\ldots,a_n)$.
Is $x \in L$, dan zijn de n+1 elementen $1,x,x^2,\ldots,x^n$ lineair afhankelijk over K, d.w.z. er zijn $a_i \in K$, niet alle 0, zodat

$$a_nx^n + \ldots + a_1x+a_0 = 0.$$

x is dus algebraïsch over K.

(5.2) <u>Stelling</u>. Is $L = K(x_1,\ldots,x_h)$ met $x_1,\ldots,x_h$ algebraïsch over K. Dan is $|L:K|$ eindig.
<u>Bewijs.</u> Met volledige inductie naar h.
$h = 1$. Dan is volgens (4.2), $|K(x_1):K| = gr(f)$, dus eindig.
Stel bewezen voor h-1. $K(x_1,\ldots,x_h) = K(x_1,\ldots,x_{h-1})(x_h)$, dus $|K(x_1,\ldots,x_h) : K(x_1,\ldots,x_{h-1})|$ is eindig.
Uit de inductieveronderstelling en (4.1) volgt dan dat $|K(x_1,\ldots,x_h) : K|$ eindig is.

(5.3) <u>Stelling</u>. Zij L een uitbreiding van K. De elementen van L die algebraïsch zijn over K vormen een deellichaam L_a van L dat K omvat.
<u>Bewijs.</u> We moeten aantonen: als x en y algebraïsch zijn over K, dan ook $x \pm y$, xy en, als $x \neq 0$, ook x^{-1}. Wegens (5.2) is $|K(x,y):K|$ eindig, dus volgens (5.1) is $K(x,y)$ algebraïsch over K. Daaruit volgt het gestelde.

L_a als in (5.3) heet de <u>algebraïsche afsluiting van K in L</u>.

(5.4) Stelling. Zij L algebraïsch over K, M algebraïsch over L. Dan is M algebraïsch over K.

Bewijs. Zij $x \in M$. x is algebraïsch over L, dus voldoet aan een vergelijking

$$a_n x^n + \dots + a_1 x + a_0 = 0$$

met $a_i \in L$. Dus is x algebraïsch over $K(a_0,\dots,a_n)$.
Dus $|K(a_0,\dots,a_n,x) : K(a_0,\dots,a_n)| < \infty$. Verder zijn $a_0,\dots,a_n$ algebraïsch over K, dus $|K(a_0,\dots,a_n) : K| < \infty$.
Daaruit volgt $|K(a_0,\dots,a_n,x) : K| < \infty$, dus x is algebraïsch over K.

Uit (5.3) en(5.4) volgt onmiddellijk:

(5.5) Stelling. Zij L_a de algebraïsche afsluiting van K in L. Is $x \in L$, $x \notin L_a$, dan is x transcendent over L_a.

Het volgende resultaat heeft een belangrijke toepassing.

(5.6) Stelling. Als $L = K[x_1,\dots,x_n]$ een lichaam is, dan is het algebraïsch over K.

Bewijs. Inductie naar n. Voor n=1 redeneren we aldus: is x_1 transcendent over K, dan $K(x_1) \cong K(X)$; $K[X] \neq K(X)$, dus $K[x_1] \neq K(x_1)$, d.w.z. $K[x_1]$ is geen lichaam: tegenspraak. Dus $K(x_1)$ is algebraïsch over K.
Stel de bewering is bewezen voor n-1. $L = K(x_1)[x_2,\dots,x_n]$, dus L is algebraïsch over $K(x_1)$. We zijn klaar als we bewijzen kunnen dat x_1 algebraïsch is over K.
Zij voor $i \geq 2$, f_i een minimumveelterm van x_i over $K(x_1)$.

$$f_i(X) = b_i X^{m_i} + c_i X^{m_i - 1} + \dots$$

Door met de noemers van b_i, c_i, ... te vermenigvuldigen, kunnen we bereiken dat alle coëfficiënten van f_i in $K[x_1]$ zitten.
Neem $y \in L$. Dan

$$y = \sum_{j_1,\dots,j_n} \alpha_{j_1,\dots,j_n} x_1^{j_1} \dots x_n^{j_n} \text{ met } \alpha_{j_1,\dots,j_n} \in K$$

$$= \sum_{j_2,\dots,j_n} \Big(\sum_{j_1} \alpha_{j_1,\dots,j_n} x_1^{j_1} \Big) x_2^{j_2} \dots x_n^{j_n} .$$

Voor $i \geq 2$ is $b_i x_i^{m_i}$ een lineaire combinatie van $x_i^{m_i - 1},\dots,x_i,1$ met coëfficiënten in $K[x_1]$.

Voor voldoende grote r is dus

$$(b_2 \ldots b_n)^r y = \Sigma\, a_{j_2,\ldots,j_n}\, x_2^{j_2} \ldots x_n^{j_n}$$

waarbij gesommeerd wordt over $j_2,\ldots,j_n$ met $0 \leq j_i < m_i$, en waarin alle $a_{j_2,\ldots,j_n} \in K[x_1]$.

Zij $1 = t_1, t_2, \ldots, t_q$ een basis van L over $K(x_1)$. Dan is

$$x_2^{j_2} \ldots x_n^{j_n} = \frac{b_{j_2\ldots j_n}}{c_{j_2,\ldots j_n}} t_1 + \ldots t_2 + \ldots..$$

met $b_{j_1,\ldots,j_n}$ en $c_{j_2,\ldots,j_n} \in K[x_1]$. Noem

$$\prod_{j_2,\ldots,j_n} c_{j_2,\ldots,j_n} = b_1 . \quad \text{Dan is}$$

$$b_1 x_2^{j_2} \ldots x_n^{j_n} = d_{j_2,\ldots,j_n} t_1 + \ldots t_2 + \ldots..$$

met $d_{j_2,\ldots,j_n} \in K[x_1]$.

Dan hebben we

$(b_1 b_2 \ldots b_n)^r y = e_1 t_1 + e_2 t_2 + \ldots + e_q t_q$

met $e_1 \in K[x_1]$, $e_2,\ldots,e_q \in K(x_1)$.

Noem $b_1 b_2 \ldots b_n = b$. Dan hebben we dus bewezen:

bij iedere $y \in L$ is er een r zodat

$$b^r y = e_1 t_1 + e_2 t_2 + \ldots + e_q t_q .$$

met $e_1 \in K[x_1]$, $e_2,\ldots,e_n$ $K(x_1)$.

Neem nu $t \in K[x_1]$, $t \neq 0$. Dan is er dus een r zodat

$$b^r t^{-1} = e_1 t_1 + e_2 t_2 + \ldots + e_q t_q .$$

$$b^r = e_1 t\, t_1 + \ldots..$$

$b^r \in K[x_1]$, dus is

$$b^r = e_1 t\, t_1 = e_1 t \quad \text{wegens } t_1 = 1.$$

Dus iedere $t \in K[x_1]$ is een deler van b^r voor voldoende grote r. Stel nu x_1 was transcendent over K. Dan waren er oneindig veel verschillende irreducibele polynomen in x_1 in $K[x_1]$, die niet alle delers van een macht van b kunnen zijn: tegenspraak. Dus moet x_1 algebraïsch zijn over K.

Als toepassing de volgende stelling.

(5.7) Stelling. ("Nullstellensatz" van Hilbert).

Zij A een echt ideaal in $K[X_1,\dots,X_n]$. Dan is er een algebraïsche uitbreiding L van K waarin elementen $x_1,\dots,x_n$ bestaan zodat $f(x_1,\dots,x_n) = 0$ voor alle $f \in A$. We noemen $(x_1,\dots,x_n)$ een nulpunt van A.

Bewijs. A ligt in een maximaal ideaal M.

$K[X_1,\dots,X_n]/M$ is een lichaam L. Noem $X_i + M = x_i$, dan is $L = K[x_1,\dots,x_n]$. Dus L is algebraïsch over K. Voor $f \in M$ is

$$f(x_1,\dots,x_n) = f(X_1,\dots,X_n) + M = 0+M = 0 \text{ in } L.$$

Opgaven.

1. Zij K een lichaam, L en M uitbreidingen van K, u een K-isomorfisme van L op M.

(i) $x \in L$ is algebraïsch over K dan en slechts dan als $u(x)$ algebraïsch is over K.

(ii) Is L algebraïsch over K, dan ook M.

2. Zij T transcendent over een lichaam K. Bewijs dat K de algebraïsche afsluiting is van K in K(T).

6. Een lichaam L heet algebraïsch gesloten als L geen algebraïsche uitbreiding toelaat.

(6.1) Stelling. Zij L een lichaam. De volgende voorwaarden voor L zijn equivalent.

(i) L is algebraïsch gesloten.

(ii) Iedere veelterm in L[X] is in lineaire factoren te ontbinden.

(iii) Iedere veelterm in L[X] heeft een wortel in L.

Bewijs. (i) $\Rightarrow$ (ii). Zij $f \in L[X]$. Ontbind f in irreducibele factoren. Het is voldoende (ii) te bewijzen voor een irreducibele veelterm. Stel f dus irreducibel. f heeft een wortel in een algebraïsche uitbreiding van L, dus in L zelf. Dus is f lineair.

(ii) $\Rightarrow$ (iii). Triviaal.

(iii) $\Rightarrow$ (i). Zij M een algebraïsche uitbreiding van L. Stel $x \in M$. Is f het minimumpolynoom van x over L, dan is f irreducibel. Anderzijds heeft f een wortel in L. Dus is f lineair, d.w.z. $x \in L$.

Zij K een lichaam. L heet een <u>algebraïsche afsluiting van K</u> als L een algebraïsch gesloten algebraïsche uitbreiding van K is.

(6.2) <u>Stelling</u>. Zij K een lichaam, M een algebraïsche uitbreiding van K en L een algebraïsche afsluiting van K. Dan is er een K-isomorfisme van M in L.
<u>Bewijs</u>. Volgens (3.13) is er een lichaam P zodat er K-isomorfismen $u: L \to P$ en $v: M \to P$ bestaan en zodat P voortgebracht is door $u(L)$ en $v(M)$. $v(M)$ is algebraïsch over K, dus zeker over $u(L)$. Dus P is algebraïsch over $u(L)$ en derhalve $P = u(L)$. $u^{-1} \circ v$ is een K-isomorfisme van M in L.

(6.3) <u>Stelling</u>. Zij K een lichaam, L en M algebraïsche afsluitingen van K. Dan is er een K-isomorfisme van L op M.
<u>Bewijs</u>. Volgens de vorige stelling is er een K-isomorfisme u van L in M. $u(L)$ is een algebraïsche afsluiting van K, M is algebraïsch over $u(L)$, dus $u(L) = M$.

(6.4) <u>Stelling</u>. Zij L een algebraïsche uitbreiding van K met de volgende eigenschap:
Voor iedere uitbreiding M van K met $|M : K| < \infty$ is er een K-isomorfisme van M in L.
Dan is L een algebraïsche afsluiting van K.
<u>Bewijs</u>. We hoeven slechts aan te tonen dat L algebraïsch gesloten is. Stel N is een algebraïsche uitbreiding van L, $x \in N, \notin L$. x is dan algebraïsch over K. Zij f het minimumpolynoom van x over K. Laat f precies $m(\geq 0)$ verschillende wortels hebben in L, zeg $y_1, \ldots, y_m$. $K(x, y_1, \ldots, y_m)$ is een uitbreiding van K van eindige graad, waarin f minstens m+1 verschillende wortels heeft.
Er is een K-isomorfisme van $K(x, y_1, \ldots, y_m)$ in L, dus f heeft minstens m+1 wortels in L: tegenspraak. Dus $N = L$.

(6.5) <u>Stelling</u>. Ieder lichaam heeft een algebraïsche afsluiting.
<u>Bewijs</u>. Zij K een lichaam. Beschouw de verzameling van alle lichamen $K[X_1, \ldots, X_m]/I$, $m = 1, 2, \ldots$, I maximaal ideaal in de polynoomring $K[X_1, \ldots, X_m]$. Volgens (3.13) is er een uitbreiding L van K waarin al deze lichamen K-isomorf ingebed zijn. Neem de algebraïsche afsluiting L_a van K in L. L_a is algebraïsch over K. Is M een uitbreiding van K met $|M : K| < \infty$, dan is

$M \cong K[X_1,\ldots,X_m]/I$ voor zekere m en zeker maximaal ideaal I. Dus M is K-isomorf af te beelden in L_α. Volgens (6.4) is L_a dan een algebraïsche afsluiting van K.

De algebraïsche afsluiting van een lichaam K noteren we meestal als $\bar{K}$. Is $\mathbb{Q}$ het lichaam van de rationale getallen, dan heet $\bar{\mathbb{Q}}$ het lichaam van de algebraïsche getallen.

Opgaven.

1. Bewijs: $\bar{\mathbb{Q}}$ heeft aftelbaar veel elementen.

2. Zij K een lichaam. Bewijs dat er in K[X] oneindig veel irreducibele polynomen zitten.

3. Zij K een eindig lichaam. Laat zien dat $\bar{K}$ aftelbaar oneindig veel elementen bevat. Een algebraïsch gesloten lichaam heeft dus altijd oneindig veel elementen.

7. Stel L is een uitbreiding van K. Elementen $x_1,\ldots,x_n$ van L heten algebraïsch afhankelijk over K als er een veelterm $f \neq 0$ in $K[X_1,\ldots,X_n]$ is met $f(x_1,\ldots,x_n) = 0$. Zijn $x_1,\ldots,x_n$ niet algebraïsch afhankelijk over K, dan heten ze algebraïsch onafhankelijk over K. Een willekeurige verzameling elementen $\{x_\alpha\}$ in L heet algebraïsch onafhankelijk over K, als iedere eindige deelverzameling van $\{x_\alpha\}$ algebraïsch onafhankelijk is.
$x \in L$ heet algebraïsch afhankelijk van $x_1,\ldots,x_n$ over K, als x algebraïsch is over $K(x_1,\ldots,x_n)$.
$x_1,\ldots,x_n$ zijn algebraïsch afhankelijk over K dan en slechts dan als er een i is zodat x_i algebraïsch afhankelijk is van $x_1,\ldots,x_{i-1}, x_{i+1},\ldots,x_n$.
Deze begrippen lijken veel op lineaire afhankelijkheid etc. uit de lineaire algebra. Men kan lineaire en algebraïsche afhankelijkheid beschrijven met eenzelfde axiomasysteem; zie Van der Waerden, Algebra.
$x_1,\ldots,x_n$ heet een transcendentiebasis van L over K, als $x_1,\ldots,x_n$ algebraïsch onafhankelijk zijn over K en iedere $x \in L$ algebraïsch afhankelijk is van $x_1,\ldots,x_n$ over K. Analoog kan men een oneindige transcendentiebasis definiëren; zie opgave 2.

(7.1) Stelling. Als $x_1,\ldots,x_n$ een transcendentiebasis is van L over K en $y_1,\ldots,y_s$ zijn algebraïsch onafhankelijk over K, dan is $s \leq n$ en er bestaan n-s elementen x_i van de gegeven basis die samen met $y_1,\ldots,y_s$ een transcendentiebasis vormen.

Bewijs. Volledige inductie naar s. Voor s=0 is er niets te bewijzen. Stel $s>0$ en neem aan dat de stelling voor s-1 i.p.v. s bewezen is. Dan is $s-1\leq n$ en er zijn $n-s+1$ elementen x_i, die met $y_1,\ldots,y_{s-1}$ een transcendentiebasis vormen; stel deze elementen zijn $x_s,x_{s+1},\ldots,x_n$. Dus $y_1,\ldots,y_{s-1}$, x_s, $x_{s+1},\ldots,x_n$ vormen een transcendentiebasis. y_s is daarvan algebraïsch afhankelijk, dus is er een niet triviale relatie

$$\sum_{i=0}^{t} a_i(y_1,\ldots,y_{s-1}, x_s,\ldots,x_n)y_s^{\,i} = 0 ,$$

met $a_i\in K[X_1,\ldots,X_n]$. Omdat $y_1,\ldots,y_s$ algebraïsch onafhankelijk zijn, moet één van de x_i echt voorkomen in deze relatie; laat dit bijv. x_s zijn. Dan is x_s algebraïsch afhankelijk van $y_1,\ldots,y_s$, $x_{s+1},\ldots,x_n$. Dus $K(y_1,\ldots,y_s, x_s, x_{s+1},\ldots,x_n)$ is een algebraïsche uitbreiding van $K(y_1,\ldots,y_s, x_{s+1},\ldots,x_n)$. Stel nu $x\in L$. Dan is x algebraïsch over $K(y_1,\ldots,y_{s-1}$, $x_s,\ldots,x_n)$, dus zeker over $K(y_1,\ldots,y_s, x_s,\ldots,x_n)$. Dan is x ook algebraïsch over $K(y_1,\ldots,y_s, x_{s+1},\ldots,x_n)$. We hoeven nog slechts aan te tonen dat $y_1,\ldots,y_s$, $x_{s+1},\ldots,x_n$ algebraïsch onafhankelijk zijn. Stel dit was niet het geval. Omdat $y_1,\ldots,y_{s-1}, x_{s+1},\ldots,x_n$ algebraïsch onafhankelijk zijn, zou dan y_s algebraïsch afhankelijk zijn van $y_1,\ldots,y_{s-1}$, $x_{s+1},\ldots,x_n$. Dan zou iedere $x\in L$ al algebraïsch afhankelijk zijn van $y_1,\ldots,y_{s-1}$, $x_{s+1},\ldots,x_n$, dus zouden $y_1,\ldots,y_{s-1}$, $x_{s+1},\ldots,x_n$ al een transcendentiebasis vormen. Maar dan was x_s algebraïsch afhankelijk van $y_1,\ldots,y_{s-1}$, $x_{s+1},\ldots,x_n$, in tegenspraak met de veronderstelling.

Een onmiddellijk gevolg van de vorige stelling is:

(7.2) Stelling. Heeft L een transcendentiebasis over K bestaande uit n elementen, dan heeft iedere transcendentiebasis van L over K precies n elementen.

Heeft L een transcendentiebasis van n elementen over K, dan heet n de transcendentiegraad van L over K; notatie : trgr(L:K). Heeft L geen eindige transcendentiebasis over K, dan stellen we $\mathrm{trgr}(L:K)=\infty$.

(7.3) Stelling. Als $K\subset L\subset M$, dan is

$$\mathrm{trgr}(M:K) = \mathrm{trgr}(M:L) + \mathrm{trgr}(L:K).$$

Bewijs. Zij $x_1,\ldots,x_r$ een transcendentiebasis van L over K , $y_1,\ldots,y_s$ één van M over L. Dan is $x_1,\ldots,x_r, y_1,\ldots,y_s$ een transcendentiebasis van M over K. Ga dit zelf na! Ga ook na dat de stelling goed is wanneer trgr(M : L) of trgr(L : K) oneindig is.

Een eindig voortgebrachte uitbreiding heeft eindige transcendentiegraad. Stel n.l $L= K(x_1,\ldots,x_n)$. Zijn de $x_1,\ldots,x_n$ algebraïsch onafhankelijk, dan vormen ze een transcendentiebasis. Zijn ze dat niet, dan is er een x_i die algebraïsch afhankelijk is van $x_1,\ldots,x_{i-1}, x_{i+1},\ldots,x_n$. Zijn ook die nog algebraïsch afhankelijk, dan laten we er weer een x_j uit weg die algebraïsch afhangt van de rest. Zo voortgaande vinden we een (eventueel leeg) stelsel algebraïsch onafhankelijke elementen $x_{i_1},\ldots,x_{i_r}$ waar de overige x_e algebraïsch van afhangen. Dus L is algebraïsch over $K(x_{i_1},\ldots,x_{i_r})$; derhalve vormen $x_{i_1},\ldots,x_{i_r}$ een transcendentiebasis. Merk nog op dat $\mathrm{trgr}(K(x_1,\ldots,x_r):K) \leq r$.

Is $\{x_\alpha\}_{\alpha\in I}$ een verzameling algebraïsch onafhankelijke elementen over K, dan heet $K(x_\alpha)_{\alpha\in I}$ een <u>zuiver transcendente</u> uitbreiding van K. Dan is $K(x_\alpha)_{\alpha\in I} \cong K(X_\alpha)_{\alpha\in I}$, het quotiëntenlichaam van de polynoomring $K[X_\alpha]_{\alpha\in I}$.

Opgaven.

1. Zijn $x_1,\ldots x_n$ en $y_1,\ldots,y_n$ transcendentiebases van L over K, dan is niet noodzakelijk $K(x_1,\ldots,x_n) = K(y_1,\ldots,y_n)$. Laat dit aan een voorbeeld zien (voor willekeurige n).

2. Zij L een uitbreiding van K, niet noodzakelijk van eindige transcendentiegraad. Bewijs: L heeft een transcendentiebasis over K. [Aanwijzing: beschouw de collectie van alle verzamelingen van algebraïsch onafhankelijke elementen in L, geordend door inclusie. Gebruik het lemma van Zorn]. L is dus een algebraïsche uitbreiding van een zuiver transcendente uitbreiding van K.

8. Zij $f\in K[X]$, α een element van een uitbreiding L van K. α heet een n-voudige wortel van f, als er een $g\in L[X]$ is zodat $f(X) = (X-\alpha)^n g(X)$. Is α n-voudige wortel met $n>1$, dan heet α meervoudige wortel.

f heeft α als meervoudige wortel in L dan en slechts dan als α een gemeenschappelijke wortel is van f en z'n afgeleide Df. Immers, is $f(X)=(X-\alpha)^n g(X)$, dan is

$$(Df)(X) = n(X-\alpha)^{n-1}g(X) + (X-\alpha)^n(Dg)(X),$$

dus $n>1$ dan en slechts dan als $X-\alpha$ een deler is van $(Df)(X)$. Stel nu f irreducibel in $K[X]$. Omdat $gr(Df) < gr(f)$, is in dit geval $(f,Df) = 1$. f kan dus alleen een wortel gemeen hebben met Df als $Df = 0$. Stel

$$f(x) = a_nX^n + a_{n-1} X^{n-1} + \dots + a_1X + a_0 .$$

Dan is

$$(Df)(X) = n\, a_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \dots + a_1 .$$

Is $f\neq 0$, dan kan $Df = 0$ alleen gelden wanneer kar.$K = p \neq 0$ en $a_k = 0$ voor alle k zodat $p\nmid k$. Dan is dus $f = a_0 + a_pX^p + a_{2p}X^{2p} + \dots$ $\dots + a_{rp} X^{rp}$. Dus hebben we

(8.1) Stelling. Zij $f\in K[X]$ irreducibel. f heeft meervoudige wortels dan en slechts dan als $kar(K) = p \neq 0$ en $f(X) = g(X^p)$ voor een $g\in K[X]$.

Heeft een irreducibel polynoom f geen meervoudige wortels, dan noemen we f separabel, anders inseparabel. Is f inseparabel, dan is $f = g(X^p)$. Is g ook weer inseparabel, dan $g(X) = h(X^p)$, dus $f(X) = h(X^{p^2})$. Zo voortgaande vinden we tenslotte een separabel polynoom f_1 zodat $f(X) = f_1(X^{p^e})$. Is α een wortel van f in L, dan is α^{p^e} een wortel van f_1. Omdat $kar(K) = p$, is $X^{p^e} - \alpha^{p^e} = (X-\alpha)^{p^e}$, dus de multipliciteit van de wortel α van f is p^e . Daarmee is bewezen :

(8.2) Stelling. Zij $kar(K) = p$, $f\in K[X]$ f irreducibel. Dan is er een separabel polynoom $f_1\in K[X]$ zodat $f(X) = f_1(X^{p^e})$. Alle wortels van f in een uitbreiding van K hebben dezelfde multipliciteit, n.l. p^e.

Zij x algebraïsch over een lichaam K. x heet separabel over K als het minimumpolynoom van x over K separabel is, anders inseparabel.

De karakteristieke exponent van een lichaam K is 1, als kar.K = 0, p als kar.K = p $\neq$ 0.

(8.3) Hulpstelling. Zij K een lichaam met karakteristieke exponent e. Dan geldt:
(i) Is (α_{ij}) een vierkante matrix met elementen in K, dan is $\det(\alpha_{ij}^{e}) = (\det(\alpha_{ij}))^{e}$.
(ii) Is (α_{ij}) een willekeurige matrix met elementen in K, dan is $\operatorname{rang}(\alpha_{ij}^{e}) = \operatorname{rang}(\alpha_{ij})$.
Bewijs. Voor e = 1 is er niets te bewijzen. Voor e = p is $\lambda \to \lambda^{p}$ een isomorfisme van K in zichzelf. Daaruit volgt (i) onmiddellijk. (ii) ziet men in door op te merken dat overeenkomstige onderdeterminanten in (α_{ij}) en (α_{ij}^{e}) tegelijkertijd 0 of $\neq$ 0 zijn.

(8.4) Stelling. Zij K een lichaam met karakteristieke exponent e, L een uitbreiding van K. De volgende uitspraken zijn equivalent.
(i) Zijn $x_1,\dots,x_n$ K-lineair onafhankelijk in L, dan ook $x_1^{e},\dots,x_n^{e}$.
(ii) L heeft een basis $\{y_\alpha\}$ over K zodat de elementen y_α^{e} lineair onafhankelijk zijn over K.
Bewijs. (i) $\Rightarrow$ (ii) : triviaal.
(ii) $\Rightarrow$ (i) : $x_1,\dots,x_n$ hangen lineair af van eindig veel y_α, zeg van $y_1,\dots,y_s$, $s \geq n$. Stel $x_i = \sum_{j=1}^{s} \alpha_{ij} y_j$.

$$x_i^{e} = \sum_j \alpha_{ij}^{e} y_j^{e} .$$

$y_1^{e},\dots,y_s^{e}$ zijn lineair onafhankelijk, en $\operatorname{rang}(\alpha_{ij}^{e}) = \operatorname{rang}(\alpha_{ij}) = n$, dus ook $x_1^{e},\dots,x_n^{e}$ zijn lineair onafhankelijk.

(8.5) Stelling. Zij K een lichaam met karakteristieke exponent e. Stel x is algebraïsch over K. De volgende uitspraken zijn equivalent.
(i) x is separabel over K.
(ii) Zijn $x_1,\dots,x_n$ K-lineair onafhankelijk in K(x), dan ook $x_1^{e},\dots,x_n^{e}$.
Bewijs. Voor e = 1 is er niets te bewijzen. Stel dus e = p.
(i) $\Rightarrow$ (ii). Zij f het minimumpolynoom van x, van graad r.

$1, x, x^2, \ldots, x^{r-1}$ vormen een basis van $K(x)$ over K. Stel , $1, x^p, x^{2p}, \ldots, x^{(r-1)p}$ zijn lineair afhankelijk over K. Er is dus een relatie

$$\lambda_0 + \lambda_1 x^p + \lambda_2 x^{2p} + \ldots + \lambda_{r-1} x^{(r-1)p} = 0,$$

met niet alle $\lambda_i = 0$. x is dus een wortel van $g(X^p)$

met $$g(X) = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \ldots + \lambda_{r-1} X^{r-1} .$$

Dus $$g(X^p) = f^s(X)\, q(X),$$ waarin q niet deelbaar is door f. De graad van $g(X^p)$ is $p(r-1)$, die van $f^s(X)$ is sr. Dus $p(r-1) \geq sr$, oftewel $(p-s)r \geq p$. Dus $1 \leq s < p$. Differentiëren van de vergelijking $g(X^p) = f^s(X)q(X)$ levert:

$$0 = s f^{(s-1)}(X).\ (Df)(X)\ q(X) + f^s(X)(Dq)(X).$$

$$f(X)\cdot(Dq)(X) = s(Df)(X)q(X).$$

Het irreducibele polynoom f is echter niet deelbaar op Df en ook niet op q : tegenspraak. Dus zijn $1, x^p, x^{2p}, \ldots, x^{(r-1)p}$ lineair onafhankelijk over K. Uit (8.4) volgt dan (ii).

(ii) $\Longrightarrow$ (i). Stel x is niet separabel over K. Het minimumpolynoom van x is dan van de gedaante $f(X^p)$ met $f(X) = = a_0 + a_1 X + \ldots + a_r X^r$. De elementen $1, x^p, x^{2p}, \ldots, x^{rp}$ zijn dus lineair afhankelijk, dus ook $1, x, x^2, \ldots, x^r$. Maar dan is x al wortel van een polynoom

$$b_0 + b_1 X + \ldots + b_r X^r ,$$

dat lagere graad heeft dan het minimumpolynoom: tegenspraak.

De voorgaande stelling leidt ons tot de volgende definitie. Een (niet noodzakelijk algebraïsche) uitbreiding L van K heet <u>separabel</u>, als geldt: zijn $x_1, \ldots, x_n$ K-lineair onafhankelijke elementen in L, dan ook $x_1^e, \ldots, x_n^e$, waarin e de karakteristieke exponent van K is. Stelling (8.4) laat zien, dat voor separabiliteit van L over K voldoende is dat L een K-basis $\{y_\alpha\}$ heeft, zodat de y_α^e een onafhankelijk stelsel vormen. Is kar.$K = 0$, dan is iedere uitbreiding van K separabel. (8.5) zegt: is x algebraïsch over K, dan is $K(x)$ separabel over K dan en slechts dan als x separabel is over K.

(8.6) Stel K, L en M zijn lichamen met $K \subset L \subset M$. e= karakteristieke exponent van K, L en M. Dan geldt:

(i) Is L separabel over K en M separabel over L, dan is M separabel over K.

(ii) Is M separabel over K, dan is L separabel over K.

(iii) Is M separabel over K en L algebraïsch over K, dan is M separabel over L.

Bewijs. (i) Zij $\{x_\alpha\}$ een basis van L over K, $\{y_\beta\}$ een basis van M over L. Dan is $\{x_\alpha y_\beta\}$ een basis van M over K. $\{x_\alpha^e\}$ is een K-lineair onafhankelijk stelsel in L, $\{y_\beta^e\}$ een L-lineair onafhankelijk stelsel in M, dus $\{(x_\alpha y_\beta)^e\}$ is een K-lineair onafhankelijk stelsel in M. Uit (8.4) volgt dat M separabel is over K.

(ii) is een triviaal gevolg van de definitie van separabiliteit.

(iii) Laat $y_1,\ldots,y_n$ L-lineair onafhankelijk zijn in M. Stel $\sum_{j=1}^{n} \lambda_j y_j^e = 0$ met $\lambda_j \in L$. De λ_j zijn algebraïsch over K, dus $|K(\lambda_1,\ldots,\lambda_n) : K| < \infty$. Wegens (ii) is $K(\lambda_1,\ldots,\lambda_n)$ separabel over K. Neem een K-basis $x_1,\ldots,x_r$ van $K(\lambda_1,\ldots,\lambda_n)$. $x_1^e,\ldots,x_r^e$ zijn dan ook een K-basis van $K(\lambda_1,\ldots,\lambda_n)$. De $x_i y_j$ zijn lineair onafhankelijk over K, dus wegens de separabiliteit van M over K zijn ook de $x_i^e\, y_j^e$ het. Er zijn $\lambda_{ij} \in K$ zodat $\lambda_j = \sum_{i=1}^{r} \lambda_{ij} x_i^e$.

Dus $\sum_{ij} \lambda_{i,j}\, x_i^e y_j^e = 0$. Maar dan zijn alle $\lambda_{i,j} = 0$, dus ook alle $\lambda_j = 0$.

De voorwaarde "L algebraïsch over K" kan niet gemist worden in (iii), zoals in opgave 2 zal blijken.

(8.7) Stelling. Zij L een algebraïsch uitbreiding van K. L is separabel over K dan en slechts dan als iedere $x \in L$ separabel is over K.

Bewijs. Stel L separabel over K. Is $x \in L$, dan $K \subset K(x) \subset L$. Dan is ook $K(x)$ separabel over K, dus x separabel over K.

Stel omgekeerd ieder element van L is separabel over K. Laat $x_1,\ldots,x_n$ K-onafhankelijke elementen zijn van L.
$K \subset K(x_1) \subset K(x_1,x_2) \subset \ldots \subset K(x_1,\ldots,x_n)$. x_i is separabel over K, dus over $K(x_1,\ldots,x_{i-1})$, dus $K(x_1,\ldots,x_i)$ is een separabele uitbreiding van $K(x_1,\ldots,x_{i-1})$. Uit (8.6)(i) volgt dus de separabiliteit van $K(x_1,\ldots,x_n)$ over K. Dus zijn $x_1^e,\ldots,x_n^e$ lineair onafhankelijk over K.

Zijn x_1 en x_2 separabel over K, dan ook $x_1 \pm x_2$, $x_1 x_2$ en x_1^{-1} (als $x_1 \neq 0$). Bekijk n.l. het lichaam $K(x_1,x_2)$: dit is separabel over K. Is L een willekeurige algebraïsche uitbreiding van K, dan vormen de $x \in L$ die separabel zijn over K, een deellichaam van L, dat K omvat, genaamd de separabele afsluiting van

K in L. In het bizonder noemen we de separabele afsluiting van K in z'n algebraïsche afsluiting $\bar{K}$ de separabele afsluiting van K. Notatie: K_s. Aangezien $\bar{K}$ op K-isomorfie na bepaald is, is ook K_s op K-isomorfie na bepaald; separabiliteit over K is n.l invariant onder K-isomorfismen.

Een lichaam K noemen we perfect, als iedere $x \in K$ te schrijven is als $x = y^e$, $y \in K$, waarin e de karakteristieke exponent van K voorstelt. Een lichaam van karakteristiek 0 is dus perfect.

(8.8) Hulpstelling. Zij kar.K = p, $a \in K$. Dan is $X^p - a$ irreducibel in K[X] of $X^p - a = (X-\alpha)^p$ met $\alpha \in K$.

Bewijs. Zij f een irreducibele factor van $X^p - a$ in K[X]. f heeft een wortel α in een algebraïsche uitbreiding L van K. In L is dus $a = \alpha^p$, dus in L[X] is $X^p - a = (X-\alpha)^p$. Is $gr(f) > 1$, dan heeft f dus meervoudige wortels, dus volgens (8.1) is $f(X) = g(X^p)$ voor een $g \in L[X]$. Dan is echter $gr(f) \geq p$, dus $f(X) = X^p - a$, op een constante na. $X^p - a$ is dus irreducibel in dit geval. Is $gr(f) = 1$, dan $\alpha \in K$.

(8.9) Stelling. De volgende uitspraken over een lichaam K zijn equivalent.

(i) K is perfect.

(ii) Iedere uitbreiding van K is separabel.

(iii) Iedere uitbreiding van K van eindige graad is separabel.

Bewijs. (i) $\Rightarrow$ (ii). Stel L is een uitbreiding van K en $x_1, \ldots, x_n$ zijn K-lineair onafhankelijk in L. Laat e de karakteristieke exponent van K zijn. Stel $\sum_{i=1}^{n} \lambda_i x_i^e = 0$ met $\lambda_i \in K$.

K is perfect, dus er zijn $\mu_i \in K$ zodat $\lambda_i = \mu_i^e$. Dan is

$(\sum_i \mu_i x_i)^e = \sum_i \mu_i^e x_i^e = 0$, dus $\sum_i \mu_i x_i = 0$. Dan moeten alle

$\mu_i = 0$ zijn, dus alle $\lambda_i = 0$.

(ii) $\Rightarrow$ (iii) is triviaal.

(iii) $\Rightarrow$ (i). Stel bij $\lambda \in K$ is er geen $\mu \in K$ met $\mu^e = \lambda$. Dan is $e \neq 1$, dus kar.K = p, e = p. Het polynoom $X^p - \lambda$ heeft geen wortels in K, dus is irreducibel in K[X]. Er is dus een uitbreiding K(x) van K zodat $X^p - \lambda$ minimumveelterm is van x. Dan is x inseparabel over K, dus K(x) inseparabel over K, in tegenspraak met (iii).

(8.10) Stelling. Ieder eindig lichaam is perfect.
Bewijs. Stel K is een eindig lichaam met karateristiek p. De afbeelding $\varphi: x \to x^p$ is een homomorfisme van K in zichzelf. Uit $x^p = 0$ volgt $x=0$, dus is φ zelfs een isomorfisme. Omdat het aantal beelden gelijk is aan het aantal elementen van K, is φ op.

We geven tenslotte een stelling over de structuur van eindig voortgebrachte separabele uitbreidingen.

(8.11) Stelling. Zij $L = K(x_1, \ldots, x_r)$. L is separabel over K dan en slechts dan als L een separabele algebraïsche uitbreiding is van een zuiver transcendente uitbreiding van K.
Bewijs. Met volledige inductie naar r bewijzen we: Is $L = K(x_1, \ldots, x_r)$ separabel over K, dan is L een separabele algebraïsche uitbreiding van een zuiver transcendente uitbreiding van K. Voor r=o valt er niets te bewijzen. Stel $r \geq 1$ en de stelling is bewezen voor $r-1$ voortbrengenden. Zijn $x_1, \ldots, x_r$ algebraïsch onafhankelijk, dan is L zuiver transcendent over K, dus dan zijn we klaar. Stel nu dat $x_1, \ldots, x_r$ algebraïsch afhankelijk zijn over K. Neem een $f \neq 0$ uit $K[X_1, \ldots, X_r]$ met minimale totale graad zodat $f(x_1, \ldots, x_r) = 0$. Stel in geval $\operatorname{kar}(K) = p$, f van de gedaante

$$f(X_1, \ldots, X_r) = g(X_1^p, \ldots, X_r^p) .$$

Dan hadden we dus een relatie

$$\Sigma\, \alpha_{i_1 \ldots i_r}\, x_1^{i_1 p} \ldots x_r^{i_r p} = 0, \quad \alpha_{i_1 \ldots i_r} \in K$$

Omdat L separabel is over K, zou er dus ook een relatie bestaan

$$\Sigma\, \beta_{i_1 \ldots i_r}\, x_1^{i_1} \ldots x_r^{i_r} = 0, \quad \beta_{i_1 \ldots i_r} \in K ,$$

niet alle $\beta_{i_1 \ldots i_r} = 0$.
Dit wil zeggen dat $x_1, \ldots, x_r$ nulpunt is van een polynoom met lagere totale graad dan f: tegenspraak. Dus is er een i, zodat X_i echt in f voorkomt maar f geen polynoom is in X_i^p en de andere X_j. Laten we aannemen dat i=1. Het voorgaande betekent dat x_1 separabel algebraïsch is over $K(x_2, \ldots, x_r)$. Volgens inductieveronderstelling is $K(x_2, \ldots, x_r)$ separabel algebraïsch over een zuiver transcendente uitbreiding van K. Hetzelfde geldt dus voor $K(x_1, \ldots, x_r)$.

Is kar(K) = 0, dan is het bewijs nog eenvoudiger.
Stel omgekeerd $K \subseteq M \subseteq L$ zodat M zuiver transcendent is over K en L algebraïsch en separabel over M. Het is voldoende aan te tonen dat M separabel is over K. Zij $y_1, \ldots, y_s$ een transcendentiebasis van M over K. Dan $M = K(y_1, \ldots, y_s) \supset K(y_1, \ldots, y_{s-1}) \supset \ldots \supset K(y_1) \supset K$. Het is voldoende aan te tonen dat $K(y_1, \ldots, y_i)$ separabel is over $K(y_1, \ldots, y_{i-1})$, d.w.z. we mogen ons beperken tot het geval s=1, dus $M = K(T)$, T transcendent over K.
Stel $x_1, \ldots, x_n \in K(T)$. $x_i = f_i g_i^{-1}$ met f_i en $g_i \in K[T]$. We kunnen iedere f_i en g_i met een factor uit K[T] vermenigvuldigen zodat alle g_i gelijk worden. Dus $x_i = f_i g^{-1}$ met f_i en $g \in K[T]$.
$x_1, \ldots, x_n$ zijn lineair onafhankelijk over K dan en slechts dan als $f_1, \ldots, f_n$ het zijn. Het is dus voldoende te bewijzen: zijn $f_1, \ldots, f_n \in K[T]$ lineair onafhankelijk over K, dan ook $f_1^p, \ldots, f_n^p$, als p = kar.K .

Stel $f_i(X) = \sum_{j=0}^{k} \alpha_{ij} X^j$ met $\alpha_{ij} \in K$. Dan $f_i^p = \sum_{j=0}^{k} \alpha_{ij}^p X^{jp}$.
Het stelsel lineaire vergelijkingen

$$\sum_{i=1}^{n} \alpha_{ij} \xi_i = 0, \quad j = 0, \ldots, k ,$$

heeft alleen de oplossing $\xi_1 = \xi_2 = \ldots = \xi_n = 0$.
Dus heeft de matrix (α_{ij}) rang n, dus ook de matrix (α_{ij}^p) heeft rang n. Daaruit volgt weer dat het stelsel

$$\sum_{i=1}^{n} \alpha_{ij}^p \xi_i = 0, \quad j = 0, \ldots, k$$

alleen de nuloplossing heeft, dus dat $f_1^p, \ldots, f_n^p$ lineair onafhankelijk zijn.

Opgaven.
1. Stel kar(K) = p, L = K(T) een transcendente uitbreiding.
Bewijs :
(i) Hetpolynoom $X^p - T \in L[X]$ heeft geen wortel in L; het is dus irreducibel (waarom?)
(ii) $X^p - T$ is een inseparabel polynoom over L.
(iii) L is niet perfect.

2. Stel kar.K = p, M = K(T), T transcendent over K. Toon aan:
(i) T^p is transcendent over K.
(ii) M is separabel over K.
(iii) M is niet separabel over $K(T^p)$.

De voorwaarde "L algebraïsch over K" kan dus niet gemist worden bij (8.6)(iii).

3. Zij kar.K = p, $L = K(t_1, t_2, \dots)$, waar t_1 transcendent is over K, $t_i^p = t_{i-1}$ voor $i > 1$. Bewijs achtereenvolgens:
(i) t_n is transcendent over K, $K(t_n) = K(t_1, t_2, \dots, t_n)$.
(ii) L is separabel over K.
(iii) $\text{trgr}(L : K) = 1$.
(iv) Is $u \in L$ transcendent over K, dan is er een n zodat $K(u) \subseteq K(t_n)$ en $|K(t_n) : K(u)| < \infty$.
(v) $K(t_{n+1})$ is niet separabel over K(u).
(vi) L is niet separabel over K(u).
(vii) L is niet te schrijven als separabele algebraïsche uitbreiding van een zuiver transcendente uitbreiding van K.
Het analogon van stelling (8.11) voor niet eindig voortgebrachte uitbreidingen geldt dus blijkbaar niet.

* 4. Stel kar(K) = p, L een algebraïsche uitbreiding van K, S de separabele afsluiting van K in L.
(i) Bewijs: Als $x \in L, \notin S$, dan is x niet separabel over S.
(ii) Zij $x \in L, \notin S$, f het minimumpolynoom van x over S. $f = g(X^{p^e})$, $g \in S[X]$ een separabel polynoom. Laat zien dat x^{p^e} separabel is over S. Wat volgt hieruit voor x^{p^e} ?
(iii) Bewijs dat $f(X) = X^{p^e} - \alpha$, $\alpha \in S$.
Een algebraïsche uitbreiding van K die geen separabele elementen buiten K bevat, noemen we zuiver inseparabel. Iedere algebraïsche uitbreiding is dus te schrijven als zuiver inseparabele uitbreiding van een separabele uitbreiding.

* 5. Zij kar.K = p. Definieer $P_n = \{x \in \bar{K} \mid x^{p^n} \in K\}$, $P = \bigcup_{n=1}^{\infty} P_n$.
Bewijs:
(i) P_n is een deellichaam van $\bar{K}$.
(ii) P is een deellichaam van $\bar{K}$.
(iii) P is perfect.
(iv) Zij P^* een minimale perfecte algebraïsche uitbreiding van K, d.w.z. een perfecte algebraïsche uitbreiding die geen perfecte algebraïsche deeluitbreidingen van K bevat die $\neq P^*$ zijn. Voor elke $x \in P^*$ is er dan een n zodat $x^{p^n} \in K$.
(v) P^* als boven. Zij u een K-isomorfisme van P^* in $\bar{K}$ (waarom is er zo'n u?). Bewijs dat $u(P^*) = P$.

Het lichaam P heet de <u>perfecte afsluiting</u> van K; het is zoals we bewezen hebben, op K-isomorfie na gekarakteriseerd door de eigenschap dat het een minimale perfecte algebraïsche uitbreiding van K is.

9. Is $f \in K[X]$, $gr(f) = n$, en L een uitbreiding van K, dan zeggen we dat <u>f splijt in L</u> (of ook wel: <u>L splijt f</u>) als er $x_1, \dots, x_n \in L$ bestaan zodat $f(X) = a(X-x_1)\dots(X-x_n)$. Is bovendien nog $L = K(x_1, \dots, x_n)$, dan heet L een <u>splijtlichaam van f</u>. Analoog voor een collectie $\{f_\alpha\}, f_\alpha \in K[X]$.

(9.1) <u>Stelling</u>. Stel $f \in K[X]$, $gr(f) = n$. Dan geldt:
(i) f heeft een splijtlichaam.
(ii) Zijn L en M splijtlichamen van f, dan zijn ze K-isomorf.
Analoog geldt voor een stel veeltermen $\{f_\alpha\}$, $f_\alpha \in K[X]$:
(iii) $\{f_\alpha\}$ heeft een splijtlichaam.
(iv) Twee splijtlichamen van $\{f_\alpha\}$ zijn altijd K-isomorf.

<u>Bewijs.</u> (i). In $\bar{K}$ zijn er $x_1, \dots, x_n$ zodat $f(X) = a(X-x_1)\dots(X-x_n)$. $K(x_1, \dots, x_n)$ is dan een splijtlichaam van f.

(ii) Er bestaan een uitbreiding N van K en isomorfismen $u : L \to N$ en $v : M \to N$. Is $L = K(x_1, \dots, x_n)$, $x_1, \dots, x_n$ wortels van f en $M = K(y_1, \dots, y_n)$, $y_1, \dots, y_n$ wortels van f, dan zijn $u(x_1), \dots, u(x_n)$, $v(x_1), \dots, v(x_n)$ wortels van f in N. Dus vormen $v(x_1), \dots, v(x_n)$ een permutatie van $u(x_1), \dots, u(x_n)$ omdat $gr(f) = n$. Dus $u(L) = v(M)$, d.w.z. $v^{-1} \circ u$ is een K-isomorfisme van L op M.

(iii) en (iv) worden analoog bewezen.

Een splijtlichaam van $f \in K[X]$ kan natuurlijk ook geconstrueerd worden zonder gebruik te maken van de algebraïsche afsluiting $\bar{K}$ van K, n.l. als volgt. Ontbind f in K[X] in irreducibele factoren. Heeft één van die factoren een graad > 1, adjungeer dan een wortel x daarvan aan K. Ontbind f dan in irreducibele factoren in K(x)[X], enz. Na eindig veel stappen heeft men een lichaam waarin f in lineaire factoren uiteenvalt; dat is dan een splijtlichaam.

Een algebraïsche uitbreiding L van K heet <u>normaal over K</u> als geldt: is f irreducibel in K[X] en heeft f een wortel in L, dan splijt f in L.

(9.2) Stelling. Stel K is een lichaam, L een uitbreiding van K met $|L:K| < \infty$. Dan zijn equivalent:

(i) L is normaal over K.

(ii) L is splijtlichaam van een $f \in K[X]$.

Bewijs. (i) $\Rightarrow$ (ii). Omdat $|L:K| < \infty$, zijn er $x_1, \dots, x_r$, algebraïsch over K, zodat $L = K(x_1, \dots, x_r)$. Zij f_i minimumpolynoom van x_i over K. f_i splijt in L. L is splijtlichaam van $f_1 f_2 \dots f_r$.

(ii) $\Rightarrow$ (i). Stel $f(X) = a(X-x_1)\dots(X-x_n)$ in L. Neem een irreducibele $g \in K[X]$ die een wortel x in L heeft. Stel g is niet in lineaire factoren te ontbinden in $L[x]$. Beschouw een irreducibele factor van g in $L[X]$ met graad > 1 en adjungeer een wortel x' daarvan aan L. x' is een wortel van g, dus g is minimumpolynoom van x' over K, maar ook van x. Dus $K(x)$ en $K(x')$ zijn beide K-isomorf met $K[X]/(g)$, d.w.z. er is een K-isomorfisme van $K(x)$ op $K(x')$. $L(x') = K(x_1, \dots, x_n, x') = K(x')(x_1, \dots, x_n)$ dus $L(x')$ is splijtlichaam van f over $K(x')$. Verder is $L = K(x_1, \dots, x_n) = K(x)(x_1, \dots, x_n)$, want $x \in L$, dus L is splijtlichaam van f over $K(x)$. Daar $K(x) \cong K(x')$, moet ook $L \cong L(x')$ (K-isomorfisme). Maar $|L(x'):K| > |L:K|$:tegenspraak.

(9.3) Stelling. Zij L een willekeurige algebraïsche uitbreiding van K. Dan zijn equivalent:

(i) L is normaal over K.

(ii) Er bestaat een stelsel $\{f_\alpha\}_\alpha, f_\alpha \in K[X]$, zodat L splijtlichaam is van $\{f_\alpha\}_\alpha$, d.w.z. L splijt elke f_α en $L = K(x_{\alpha,i})_{\alpha,i}$ waarin $x_{\alpha,1}, \dots, x_{\alpha,n_\alpha}$ de wortels van f_α in L zijn.

Bewijs. (i) $\Rightarrow$ (ii). Voeg aan iedere $x \in L, \notin K$, z'n minimum veelterm f_x over K toe. L is splijtlichaam van het stelsel $\{f_x\}_{x \in L, \notin K}$.

(ii) $\Rightarrow$ (i). Stel de irreducibele $g \in K[X]$ heeft een wortel $x \in L$. Er zijn dan eindig veel f_α's, zeg $f_1, \dots, f_r$, zodat $x \in K(x_{1,1}, x_{1,2}, \dots, x_{1,n}, x_{2,1}, \dots, x_{r,n_r}) = M$. Volgens de vorige stelling is M normaal over K, want M is splijtlichaam van $f_1 \cdot f_2 \cdot \dots \cdot f_r$. g splijt in M, dus zeker in L.

(9.4) Stelling. Is $K \subset L \subset M$, M normaal over K, dan is M normaal over L.

Bewijs. Stel g is irreducibel in L[X] en heeft een wortel x in M. Zij f minimum veelterm van x over K, M is normaal over K, dus f valt in lineaire factoren uiteen in M[X]. g is een deler van f, dus g valt ook in lineaire factoren uiteen in M[X].

Stel L is algebraïsch over K en M is een algebraïsche uitbreiding van L met de volgende eigenschappen: (i) M is normaal over K; (ii) is $L \subseteq N \subseteq M$, N normaal over K, dan is N=M. M heet dan een normale afsluiting van L over K.

(9.5) Stelling. Zij L een algebraïsche uitbreiding van K. Dan geldt:
(i) Er bestaat een normale afsluiting van L over K.
(ii) Twee normale afsluitingen van L over K zijn altijd isomorf.
(iii) Is $|L:K| < \infty$ en M een normale afsluiting van L over K, dan $|M:K| < \infty$.

Bewijs. (i) Beschouw voor elke $x \in L, \notin K$, de minimumveelterm over K. Neem voor M het splijtlichaam van de collectie veeltermen $\{f_x | x \in L, x \notin K\}$. M is dan klaarblijkelijk een kleinste uitbreiding van L die normaal is over K, d.w.z een normale afsluiting.

(ii) Stel M is een normale afsluiting van L over K. De veeltermen f_x als in 't bewijs van (i) splijten in M. Anderzijds is het splijtlichaam van $\{f_x | x \in L, \notin K\}$ binnen M een normale uitbreiding van K, dus gelijk aan M. Zij nu N een andere normale afsluiting van L over K. Er bestaat een uitbreiding P van L waarin M en N L-isomorf afgebeeld worden door L-isomorfismen u resp. v. u(M) en v (N) zijn splijtlichamen van het stelsel $\{f_x | x \in L, \notin K\}$ binnen P, dus moeten samenvallen: $u(M) = v(N)$. Dus $v^{-1} \circ u$ is een L-isomorfisme van M op N.

(iii) Als $|L:K| < \infty$, dan is L te schrijven als $L=K(x_1, \ldots, x_n)$, x_i algebraïsch over K. Zij f_i de minimumveelterm van x_i over K. Het splijtlichaam van $f_1 f_2 \ldots f_n$ over L is ook splijtlichaam over K, dus een normale afsluiting van L over K met eindige graad.

Opgaven.

1. Bewijs dat $\mathbb{Q}(\sqrt{2})$ een normale uitbreiding is van $\mathbb{Q}$ en $\mathbb{Q}(\sqrt[4]{2})$ een normale uitbreiding van $\mathbb{Q}(\sqrt{2})$. Toon dan aan dat $\mathbb{Q}(\sqrt[4]{2})$ geen normale uitbreiding van $\mathbb{Q}$ is.

2. Bepaal het splijtlichaam van X^3-3 over $\mathbb{Q}$. Eveneens over $\mathbb{F}_7 (= \mathbb{Z}/(7))$.

3. Zij $f \in K[X]$, $gr(f)=n$, L het splijtlichaam van f over K. Bewijs dat $|L:K| \leq n!$.

10. We bewijzen nu een aantal stellingen over automorfismen van algebraïsche uitbreidingen.

(10.1) Lemma. Zij M een normale uitbreiding van K, σ een K-isomorfisme van M in zichzelf. Dan is $\sigma(M) = M$.

Bewijs. $M = K(\{x_\alpha\})$, waarin $\{x_\alpha\}$ een stelsel elementen van M is. Zij f_α het minimumpolynoom van x_α over K. M is splijtlichaam van het stelsel $\{f_\alpha\}$ over K. $\sigma(M)$ is dus ook splijtlichaam van $\{f_\alpha\}$ over K; aangezien $\sigma(M) \subseteq M$, is zelfs $\sigma(M)=M$.

(10.2) Stelling. $K \subseteq L \subseteq M$ lichamen, M normaal over K. Stel σ is een K-isomorfisme van L in M. Dan is σ uit te breiden tot een K-automorfisme van M.

Bewijs. Beschouw paren (N,φ) , waarin N een lichaam is, $L \subseteq N \subseteq M$, en φ een K-isomorfisme van N in M zodat voor $x \in L$: $\varphi(x) = \sigma(x)$. Laat S de verzameling van al zulke paren (N,φ) zijn. $S \neq \emptyset$, want $(L,\sigma) \in S$. S wordt als volgt geordend:
$(N_1,\varphi_1) \leq (N_2,\varphi_2) \Leftrightarrow N_1 \subseteq N_2$, voor $x \in N_1$ is $\varphi_1(x) = \varphi_2(x)$.
Zij T een totaal geordende deelverzameling van S. Definieer $N_0 = \bigcup_{(N,\varphi)\in T} N$; N_0 is een deellichaam van M.
Het K-isomorfisme φ_0 van N_0 in M definiëren we als volgt: is $x \in N_0$, dan is er een $(N,\varphi) \in T$ zodat $x \in N$; dan $\varphi_0(x) = \varphi(x)$. Is tevens $x \in N_1$ met $(N_1,\varphi_1) \in T$, dan is $(N,\varphi) \leq (N_1,\varphi_1)$ of $(N_1,\varphi_1) \leq (N,\varphi)$. In beide gevallen is $\varphi(x) = \varphi_1(x)$, m.a.w. de definitie van φ_0 is ondubbelzinnig. Voor $x \in L$ is $\varphi(x) = \sigma(x)$. (N_0,φ_0) is een bovengrens van T in S. We kunnen dus het lemma van Zorn toepassen. Zij (M',φ) een maximaal element van S. We zijn klaar als we bewijzen kunnen dat $M' = M$. Stel $M' \neq M$. Neem $x \in M$, $\notin M'$. Laat f de minimumveelterm van x over K zijn, g die van x over M'. g is een deler van f. Definieer $\varphi(g)$ als volgt:

$$g(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 ,$$

$$\varphi(g)(X) = \varphi(a_n) X^n + \varphi(a_{n-1}) X^{n-1} + \ldots + \varphi(a_1) X + \varphi(a_0).$$

$\varphi(g)$ is een deler van $\varphi(f)$; omdat de coëfficiënten van f in K

zitten, is $\varphi(f) = f$. Dus: $\varphi(g)$ deelt f. f heeft een wortel in M, n.l. x, dus splijt in M(M normaal!). Dus heeft $\varphi(g)$ een wortel y in M. Zet nu φ tot $M'(x)$ voort door te definiëren

$$\psi(b_0+b_1x+\ldots+b_{n-1}x^{n-1}) = \varphi(b_0)+\varphi(b_1)y+\ldots+\varphi(b_{n-1})y^{n-1} .$$

Dan is $(M'(x), \psi) \in S$ $(M'(x), \psi) \succ (M,\varphi)$: tegenspraak met de maximaliteit van (M',φ). Dus is $M' = M$.

Opmerking : is $|M : L|$ eindig, dan heeft men 't lemma van Zorn niet nodig. Men schrijft dan $M = L(x_1,\ldots,x_r)$ en zet σ eerst voort tot $L(x_1)$, vervolgens tot $L(x_1)(x_2) = L(x_1,x_2)$, enzovoort.

(10.3) Stelling. $K \subseteq L \subseteq M$ lichamen, M algebraïsch over K. Dan geldt:
(i) Is L normaal over K, dan geldt voor ieder K-automorfisme σ van M dat $\sigma(L) = L$.
(ii) Is M normaal over K en geldt voor ieder K-automorfisme σ van M dat $\sigma(L) = L$, dan is L normaal over K.

Bewijs. (i) Neem $x \in L$. Zij f de minimumveelterm van x over K.

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 .$$

Dan $f(x) = 0$, dus $\sigma(f(x)) = 0$, d.w.z.

$$a_n\, \sigma(x)^n + \ldots + a_1 \sigma(x) + a_0 = 0.$$

Dus $\sigma(x)$ is een wortel van f in M. Daar L normaal is over K, splijt f in L; dus $\sigma(x)$ moet in L liggen. Derhalve is $\sigma(L) \subseteq L$, dus $\sigma(L) = L$.

(ii) Stel L is niet normaal over K. Dan is er een irreducibele $f \in K[X]$, die een wortel x in L heeft, maar niet splijt in L. M is normaal over K, dus f splijt wel in M. Zij $y \in M, \notin L$ een wortel van f. Dan $K(y) \cong K[X]/(f) \cong K(x)$, d.w.z. er is een K-isomorfisme $\sigma: K(x) \to K(y)$ met $\sigma(x) = y$. σ kan worden voortgezet tot een K-automorfisme τ van M. Omdat $\tau(x) = y \notin L$, is $\tau(L) \neq L$, in tegenspraak met de aanname. Dus moet L normaal zijn over K.

(10.4) Stelling. Zij L een algebraïsche uitbreiding van K. De volgende beweringen zijn equivalent:
(i) L is normaal en separabel over K.
(ii) Is $x \in L$ zodat $\sigma(x) = x$ voor iedere K-automorfisme σ van L, dan is $x \in K$.

Bewijs. (i) $\Rightarrow$ (ii). Neem $x \in L, \notin K$. Zij f de minimumveelterm van x over K. $gr(f) > 1$. L is normaal en separabel over K, dus f

heeft een wortel $y \neq x$ in M. Er is een K-isomorfisme $\sigma : K(x) \to K(y)$ met $\sigma(x) = y$. σ kan worden voortgezet tot een K-automorfisme τ van L. $\tau(x) \neq x$.

(ii) $\Longrightarrow$ (i). Stel f irreducibel in K[X] en x een wortel van f in L. We moeten aantonen dat f in L in verschillende lineaire factoren uiteenvalt. Laten $x = x_1, x_2, \ldots, x_n$ de verschillende beelden van x zijn onder alle K-automorfismen van M. Iedere x_i is een wortel van f, dus $n \leq gr(f)$.

Beschouw nu de veelterm

$$g(X) = (X-x_1)(X-x_2) \ldots (X-x_n)$$
$$= X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$
$$a_{n-i} = (-1)^i \sum_{j_1<j_2<\ldots<j_i} x_{j_1} x_{j_2} \ldots x_{j_i}$$

Zij σ een K-automorfisme van M. σ permuteert de x_i, dus

$$\sigma(a_{n-i}) = (-1)^i \sum_{j_1<\ldots<j_i} \sigma(x_{j_1}) \ldots \sigma(x_{j_i})$$
$$= (-1)^i \sum_{k_1<\ldots<k_i} x_{k_1} \ldots x_{k_i} \quad .$$
$$= a_{n-i} \; .$$

Volgens de veronderstelling is dus $a_{n-i} \in K$.
Dus $g \in K[X]$. $g(x) = 0$, dus $f | g$. Maar $gr(g) = n \leq gr(f)$, dus $f = a\,g$, $a \in K$. Daaruit volgt dat f in L in verschillende lineaire factoren uiteenvalt.

Is K een lichaam, dan duiden we met K^* de vermenigvuldigingsgroep aan van de elementen $\neq 0$ van K.
Zij G een willekeurige groep. Onder een <u>karakter van G in K</u> verstaan we een homomorfisme van G in K^*.
Voorbeeld: $G = \mathbb{Z}$, de optelgroep van de gehele getallen, $K = \mathbb{C}$, het lichaam van de complexe getallen. Is $z \in \mathbb{C}^*$, dan is χ met $\chi(n) = z^n$ een karakter van $\mathbb{Z}$ in $\mathbb{C}$.

(10.5) <u>Stelling</u>. G een groep, K een lichaam. Stel dat $\chi_1, \ldots, \chi_n$ n verschillende karakters zijn G in K. Dan zijn $\chi_1, \ldots, \chi_n$ lineair onafhankelijk over K, d.w.z. uit $\lambda_1\chi_1(g) + \ldots + \lambda_n\chi_n(g) = 0$ voor alle $g \in G$, met $\lambda_1, \ldots, \lambda_n \in K$, volgt: $\lambda_1 = \ldots = \lambda_n = 0$.

<u>Bewijs.</u> Met volledige inductie naar n.
$n=1$: $\lambda\,\chi(g) = 0$ impliceert $\lambda = 0$, daar $\chi(g) \neq 0$.

Veronderstel dat $n > 1$ en dat de stelling bewezen is voor $n-1$ karakters. Stel $\lambda_1\chi_1(g)+ \dots +\lambda_n\chi_n(g) = 0$ voor alle g. Dan is ook wegens $\chi_i(gh) = \chi_i(g)\,\chi_i(h)$,

$$\lambda_1\chi_1(g)\chi_1(h) + \lambda_2\chi_2(g)\chi_2(h)+\dots+ \lambda_n\chi_n(g)\chi_n(h) = 0.$$

Maar tevens is

$$\lambda_1\chi_1(g)\chi_1(h) + \lambda_2\chi_2(g)\chi_1(h)+\dots+ \lambda_n\chi_n(g)\chi_1(h) = 0.$$

Aftrekken geeft

$$\lambda_2(\chi_2(h)-\chi_1(h))\chi_2(g)+\dots+ \lambda_n(\chi_n(h)-\chi_1(h))\chi_n(g) = 0.$$

Uit de inductieveronderstelling volgt

$$\lambda_2(\chi_2(h)-\chi_1(h)) = \dots = \lambda_n(\chi_n(h)-\chi_n(h)) = 0.$$

Bij elke $i > 1$ is er een h zodat $\chi_i(h)-\chi_1(h) \neq 0$, want $\chi_i \neq \chi_1$. Dus is $\lambda_2 = \dots = \lambda_n = 0$. Dan ook $\lambda_1 = 0$.

Een toepassing hiervan is

(10.6) Stelling van Dedekind. Zijn L en K lichamen en $\sigma_1,\dots,\sigma_n$ verschillende isomorfismen van L in K. Dan zijn $\sigma_1,\dots,\sigma_n$ K-lineair onafhankelijk, d.w.z. uit $\lambda_1\sigma_1(x)+\dots+\lambda_n\sigma_n(a) = 0$ voor alle $x \in L$, volgt $\lambda_1 = \dots = \lambda_n = 0$.

Bewijs. Pas (10.5) toe op de karakters $\sigma_1,\dots,\sigma_n$ van L^* in K.

De stelling van Dedekind wordt vooral toegepast op automorfismen van een lichaam.

Is $\{\sigma_\alpha\}$ een collectie automorfismen van een lichaam L, dan noemt met het lichaam $K = \{x \in L \mid \sigma_\alpha(x) = x \text{ voor alle } \alpha\}$ het invariantenlichaam van $\{\sigma_\alpha\}$. Notatie: $\mathrm{Inv}(\{\sigma_\alpha\})$, of bij een eindig aantal automorfismen, $\mathrm{Inv}(\sigma_1,\dots,\sigma_n)$. Is V een eindige verzameling, dan duiden we het aantal elementen in V aan met $|V|$, vaak de orde van V genaamd.

(10.7) Stelling. Zij L een lichaam. Dan geldt:

(i) Zijn $\sigma_1,\dots,\sigma_n$ verschillende automorfismen van L, $K = \mathrm{Inv}(\sigma_1,\dots,\sigma_n)$, dan is $|L : K| \geq n$.

(ii) Is G een eindige groep van automorfismen van L, $K = \mathrm{Inv}(g)$, dan is $|L : K| = |G|$.

Bewijs. (i) Neem aan dat $|L:K|$ eindig is - anders valt er niets te bewijzen. Zij $a_1,\dots,a_r$ een basis van L over K. Stel $\lambda_1,\dots,\lambda_n \in L$ zodat

(*) $$\sum_{i=1}^{n} \lambda_i\sigma_i(a_j) = 0, \quad j=1,\dots,r.$$

Voor willekeurige $a = \alpha_1 a_1 + \ldots + \alpha_r a_r \in L$, met $\alpha_j \in K$, geldt dan

$$\sum_i \lambda_i \sigma_i(a) = \sum_j \alpha_j \sum_i \lambda_i \sigma_i(a_j) = 0.$$

Volgens de stelling van Dedekind zijn dan alle $\lambda_i = 0$. Het stelsel (*) heeft dus alleen de nuloplossing. Daaruit volgt dat $r \geq n$.

(ii) Uit (i) volgt al $|L : K| \geq |G|$.

Stel $a_1, \ldots, a_r$ K-lineair onafhankelijk in L. Beschouw het stelsel vergelijkingen voor $\lambda_j \in L$:

$$(**) \qquad \sum_{j=1}^{r} \lambda_j \sigma_i(a_j) = 0, \quad i = 1, \ldots, n.$$

We zullen aantonen dat dit alleen de nuloplossing heeft. Daaruit volgt $r \leq n$. Dus moet ook $|L : K| \leq |G|$ zijn, dus $|L : K| = |G|$. We passen inductie naar r toe. Voor $r=1$: $\lambda_1 \sigma_i(a_1) = 0$. $\sigma_i(a_1) \neq 0$, dus $\lambda_1 = 0$. Stel de bewering geldt voor $r-1$ onafhankelijke a_j, met $r > 1$. Omdat de automorfismen σ_i een groep vormen, geldt (**) ook met $\sigma_k^{-1}\sigma_i$ i.p.v. σ_i. Dus

$$\sum_{j=1} \lambda_j \sigma_k^{-1} \sigma_i(a_j) = 0 ,$$

Laat hierop σ_k werken:

$$\sum_{j=1}^{r} \sigma_k(\lambda_j) \sigma_i(a_j) = 0.$$

Vermenigvuldigen met λ_r geeft:

$$\lambda_r \sigma_k(\lambda_1)\sigma_i(a_1) + \lambda_r \sigma_k(\lambda_2) \sigma_i(a_2) + \ldots + \lambda_r \sigma_k(\lambda_r)\sigma_i(a_r) = 0.$$

Vermenigvuldigen van (**) met $\sigma_k(\lambda_r)$ geeft:

$$\lambda_1 \sigma_k(\lambda_r)\sigma_i(a_1) + \lambda_2 \sigma_k(\lambda_r) \sigma_i(a_2) + \ldots + \lambda_r \sigma_k(\lambda_r)\sigma_i(a_r) = 0.$$

Trekken we de laatste vergelijking af van de voorlaatste:

$$(\lambda_r \sigma_k(\lambda_1) - \lambda_1 \sigma_k(\lambda_r))\sigma_i(a_1) + \ldots\ldots$$

$$\ldots\ldots + (\lambda_r \sigma_k(\lambda_{r-1}) - \lambda_{r-1} \sigma_k(\lambda_r)) \sigma_i(a_{r-1}) = 0.$$

Dit geldt voor $i=1,\ldots,n$, dus uit de inductieveronderstelling volgt:

$$\lambda_r \sigma_k(\lambda_j) = \lambda_j \sigma_k(\lambda_r) , \quad j=1,\ldots,n-1.$$

Noem $\lambda_j \lambda_r^{-1} = \mu_j$. Dan is dus

$$\mu_j = \sigma_k(\mu_j), \text{ voor alle } \sigma_k \in G.$$

Dus $\mu_j \in K$. $\lambda_j = \mu_j \lambda_r$, dus schrijven we (**) op voor $\sigma_i = 1$, het eenheidselement van G, dan krijgen we

$$\lambda_r \sum_{j=1}^{r} \mu_j a_j = 0.$$

Omdat $a_1,\dots,a_r$ K-lineair onafhankelijk zijn, volgt hieruit: $\mu_1=\dots=\mu_r=0$, dus $\lambda_1=\dots=\lambda_r=0$, of $\lambda_r=0$. In het laatste geval hebben we

$$\sum_{j=1}^{r-1} \lambda_j \sigma_i(a_j) = 0, \quad i=1,\dots,n ,$$

zodat uit de inductieveronderstelling volgt dat ook $\lambda_1=\dots=\lambda_{r-1}=0$.

Opgaven.

1. Schrijf een bewijs met volledige inductie op van stelling (10.2) voor het geval dat $|M:L| < \infty$.

2. Zij M het splijtlichaam van X^4-2 over $\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2})$. Zij σ het $\mathbb{Q}$-isomorfisme van L in M, met $\sigma(\sqrt{2})=-\sqrt{2}$. Zet σ voort tot een automorfisme van M.

3. Beschouw de algebraïsche afsluiting $\bar{\mathbb{F}}_p$ van $\mathbb{F}_p$, het priemlichaam van karakteristiek p. $\sigma : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$ is het isomorfisme dat $x \to x^p$.

(i) Bewijs dat $\sigma(\bar{\mathbb{F}}_p) = \bar{\mathbb{F}}_p$, m.a.w., σ is een automorfisme van $\bar{\mathbb{F}}_p$.

(ii) Laat zien dat $Inv(\sigma) = \mathbb{F}_p$. In dit geval is dus $|\bar{\mathbb{F}}_p : Inv(\sigma)| = \infty$.

=======

Hoofdstuk III. Galoistheorie.

11. Zij T een geordende verzameling. Zijn a en b $\in$ T, dan heet c een grootste ondergrens van a en b als

(i) $c \le a$ en $c \le b$;

(ii) uit $x \le a$ en $x \le b$ volgt $x \le c$.

Is d ook een grootste ondergrens van a en b, dan c=d. Immers $d \le a$ en $d \le b$, dus $d \le c$; om dezelfde reden is $c \le d$. Dus c=d. Hebben a en b een grootste ondergrens, dan noteren we die $a \wedge b$. Analoog definiëren we de kleinste bovengrens e van a en b:

(i') $e \ge a$ en $e \ge b$;

(ii') uit $x \ge a$ en $x \ge b$ volgt $x \ge e$.

a en b kunnen hoogstens één kleinste bovengrens hebben;

notatie: $a \vee b$.
Is bijv. T de verzameling van alle deelverzamelingen van een verzameling X, met de inclusie als ordening, dan is voor A en $B \in T$, $A \wedge B = A \cap B$, de doorsnede van A en B, en $A \vee B = A \cup B$, de vereninging van A en B.

$0 \in T$ heet een nulelement van T, als $0 \leq x$ voor alle $x \in T$. Als ook $0'$ een nulelement van T is, dan $0 \leq 0'$, anderzijds $0' \leq 0$, dus $0 = 0'$. Een éénelement is een $1 \in T$ zodat $1 \geq x$ voor alle x; T kan hoogstens één éénelement hebben. $0 \wedge x = 0$, $0 \vee x = x$, $1 \wedge x = x$, $1 \vee x = 1$ voor alle $x \in T$.
Een tralie is een geordende verzameling, die een nul- en een éénelement heeft en waarin voor iedere a en b ook $a \wedge b$ en $a \vee b$ bestaan.

Zijn T en U tralies, dan heet een afbeelding $\varphi : T \to U$ een isomorfisme van T op U, als φ een afbeelding op is en als voor x en $y \in T$: $x \leq y \Leftrightarrow \varphi(x) \leq \varphi(y)$. Ga na dat φ 1-1 is, $\varphi(0) = 0$, $\varphi(1) = 1$ en dat de inverse van een isomorfisme ook een isomorfisme is. Het product van twee isomorfismen - als 't bestaat - is weer een isomorfisme. De isomorfismen van een tralie op zichzelf vormen een groep.

Een afbeelding ψ van T op U heet een anti-isomorfisme, als voor alle x en y in T geldt: $x \leq y \Leftrightarrow \psi(x) \geq \psi(y)$.
Ψ is dan ook 1-1, $\psi(0) = 1$, $\psi(1) = 0$. De inverse van een anti-isomorfisme is een antiisomorfisme.

12. Een normale en separabele lichaamsuitbreiding noemen we een Galoisuitbreiding. Zij L algebraïsch over K. De groep van K-automorfismen van L noemen we de Galoisgroep van L over K; notatie: $G_{L/K}$. Volgens (10.4) is L dan en slechts dan een Galoisuitbreiding van K, als $K = \mathrm{Inv}(G_{L/K})$. Voor een Galoisuitbreiding L van K met $|L : K| < \infty$ is volgens (10.7): $|L : K| = |G_{L/K}|$.

(12.1) Stelling. Zij $K \subset M \subset L$, L een Galoisuitbreiding van K. Dan is:
(i) L een Galoisuitbreiding van M.
(ii) $G_{L/M}$ een ondergroep van $G_{L/K}$.
(iii) M is normaal over K dan en slechts dan als $G_{L/M}$ een normaaldeler is in $G_{L/K}$.
(iv) Is M normaal over K (dus een Galoisuitbreiding van K),

dan is $G_{M/K} \cong G_{L/K} / G_{L/M}$.

Bewijs. (i) volgt uit (8.7) en (9.4)

(ii) is triviaal.

(iii) Zij $\sigma \in G_{L/M}$ en $\tau \in G_{L/K}$. $\tau \sigma \tau^{-1}$ laat alle elementen van τM vast. Dus

$$\tau G_{L/M} \tau^{-1} \subseteq G_{L/\tau M} .$$

Maar dan is ook

$$\tau^{-1} G_{L/\tau M} \tau \subseteq G_{L/\tau^{-1}\tau M} = G_{L/M} ,$$

d.w.z.

$$G_{L/\tau M} \subseteq \tau G_{L/M} \tau^{-1} .$$

Dus

$$G_{L/\tau M} = \tau G_{L/M} \tau^{-1} .$$

L is een Galoisuitbreiding van M, dus $M = \mathrm{Inv}(G_{L/M})$.

We vinden dus:

voor alle $\tau \in G_{L/K}$ is $\tau M = M \Leftrightarrow$

$$\tau G_{L/M} \tau^{-1} = G_{L/M} \text{ voor alle } \tau \in G_{L/K} ,$$

m.a.w.

M is een Galoisuitbreiding van K

$\Leftrightarrow$ $G_{L/M}$ is normaaldeler in $G_{L/K}$.

Daar M, als deellichaam van L, altijd separabel is over K, is M een Galoisuitbreiding van K dan en slechts dan als M normaal is over K. Daarmee is het gestelde bewezen.

(iv) Is $\sigma \in G_{L/K}$ en M normaal over K, dan $\sigma M = M$. Zij σ' de restrictie van σ tot M.

$\sigma \to \sigma'$ is een homomorfisme van $G_{L/K}$ in $G_{M/K}$. Volgens (10.2) is het een afbeelding op. $\sigma' = 1$ is equivalent met $\sigma \in G_{L/M}$.

Dus $G_{M/K} \cong G_{L/K} / G_{L/M}$.

(12.2) Hulpstelling. Zij L een separabele uitbreiding van K. De normale afsluiting van L over K is dan een Galoisuitbreiding van K. I.h.b. is dus voor $|L : K| < \infty$, L bevat in een Galoisuitbreiding M van K met $|M : K| < \infty$.

Bewijs. Is $L = K(\{x_\alpha\})$, f_α minimumveelterm van x_α over K, dan is de normale afsluiting M van L over K splijtlichaam van de f_α, dus separabel. Is $|L : K| < \infty$, dan $|M : K| < \infty$ zoals we gezien hebben.

(12.3) Stelling. Zij $K \subset L \subset M$, M een Galoisuitbreiding van K. Het aantal K-isomorfismen van L in M bedraagt dan $|L:K|$ (die eventueel ∞ mag zijn).

Bewijs. Zij N de normale afsluiting van L over K; we mogen aannemen dat $N \subseteq M$. Is σ een K-isomorfisme van L in M, dan is σ voort te zetten tot een K-automorfisme τ van M. Dan is $\tau N = N$, dus $\sigma L \subseteq N$. We mogen dus zonder bezwaar aannemen dat $M = N$. Stel nu eerst $|L:K| < \infty$; dan ook $|M:K| < \infty$. Zij V de verzameling van K-isomorfismen van L in M. Beschouw de afbeelding $\varphi : G_{M/K} \to V$ gedefinieerd door $\sigma \to \sigma_L$ = restrictie van σ tot L. Wegens (10.2) is dit een afbeelding op V. $\sigma_L = \tau_L \Leftrightarrow (\sigma^{-1}\tau)_L = 1 \Leftrightarrow \sigma^{-1}\tau \in G_{M/L}$. Dus φ induceert een 1-1 afbeelding van $G_{M/K}/G_{M/L}$ op V. (N.B.: Is H een ondergroep van een groep G, dan bedoelen we met G/H de verzameling van linkernevenklassen van H in G). Dus $|V| = |G_{M/K}| : |G_{M/L}| = |M:K| : |M:L| = |L:K|$. Is $|L:K| = \infty$, dan is er een oneindige rij separabele uitbreidingen K_i, $K \subset K_1 \subset K_2 \subset \dots \subset L$, met $|K_i : K| \geq i$. Ieder K-isomorfisme van K_i in M is voort te zetten tot een automorfisme van M, dus zeker tot een K-isomorfisme van L in M. Het aantal K-isomorfismen van L in M is dus $\geq |K_i : K| \geq i$ voor alle i, dus is oneindig. N.B.: We differentiëren ∞ niet nader in machtigheden. Zou men met machtigheden gaan werken, dan is bovenstaande stelling onjuist in het oneindige geval.

(12.4) Stelling. Zij $K \subset L \subset M$, $|L:K| = n$, M een Galoisuitbreiding van K. Laat $\sigma_1, \dots, \sigma_n$ de verschillende K-isomorfismen van L in M zijn en $a_1, \dots, a_n$ een K-basis van L. Dan is $\det(\sigma_i(a_j))_{1 \leq i,j \leq n} \neq 0$.

Bewijs. Stel $\det(\sigma_i(a_j)) = 0$. Dan waren er $\lambda_i \in M$, niet alle 0, zodat

$$\sum_{i=1}^{n} \lambda_i \sigma_i(a_j) = 0 , \quad j = 1, \dots, n .$$

Zij x willekeurig in L. Dan

$$x = \xi_1 a_1 + \dots + \xi_n a_n , \quad \xi_i \in K.$$

Dus

$$\sum_{i=1}^{n} \lambda_i \sigma_i(x) = \sum_{i,j} \lambda_i \xi_j \sigma_i(a_j)$$

$$= \sum_j \xi_j \left(\sum_i \lambda_i \sigma_i(a_j) \right)$$

$$= 0 .$$

Dit is in strijd met de stelling van Dedekind (10.6) .

13. We gaan nu eerst nader in op de structuur van Galoisuitbreidingen van eindige graad. Zij dus L een Galoisuitbreiding van K met $|L:K| < \infty$. De verzameling van alle ondergroepen van $G = G_{L/K}$ ordenen we door inclusie. Het is dan een tralie. Zijn H_1 en H_2 ondergroepen van G, dan is $H_1 \wedge H_2 = H_1 \cap H_2$ en $H_1 \vee H_2 = H_1 H_2$, de door H_1 en H_2 in G voortgebrachte ondergroep. Als nulelement fungeert (1), de ondergroep bestaande uit alleen het eenheidselement van G, als éénelement in de tralie fungeert G zelf. We noteren deze tralie van ondergroepen van $G = G_{L/K}$ met $\underline{\underline{G}}$ of $\underline{\underline{G}}_{L/K}$.

We introduceren nu nog een andere tralie, $\underline{\underline{L/K}}$. Elementen van $\underline{\underline{L/K}}$ zijn de lichamen M, $K \subseteq M \subseteq L$. Als ordening nemen we de inclusie. Voor M_1 en $M_2 \in \underline{\underline{L/K}}$ is $M_1 \wedge M_2 = M_1 \cap M_2$, $M_1 \vee M_2 = M_1 M_2$ in L, als $M_1 M_2$ het door M_1 en M_2 voortgebrachte deellichaam van L aanduidt.

(13.1) <u>Hoofdstelling van de Galoistheorie (eindige graad)</u>. Zij L een Galoisuitbreiding van K, $|L:K| < \infty$.

De afbeeldingen

$$g : \underline{\underline{L/K}} \rightarrow \underline{\underline{G}}_{L/K}$$

gedefinieerd door

$$g(M) = G_{L/M}$$

en

$$i : \underline{\underline{G}}_{L/K} \rightarrow \underline{\underline{L/K}}$$

gedefinieerd door

$$i(H) = \mathrm{Inv}(H)$$

zijn anti-isomorfismen op, en wel elkaars inverse.

<u>Bewijs.</u> Is $M \in \underline{\underline{L/K}}$, dan is wegens (10.4) (ii) ,

$$M = \mathrm{Inv}(G_{L/M}) = i \circ g(M).$$

Dus $i \circ g = 1.$

Stel omgekeerd $H \in \underline{\underline{G}}_{L/K}$. Duidelijk is dat

$$g \circ i(H) \geq H.$$

Anderzijds is

$$|g \circ i(H)| = |L : i(H)| = |H| ,$$

dus
$$g \circ i(H) = H,$$
$$g \circ i = 1.$$

i en g zijn dus 1-1 en op en elkaars inverse. Daar i en g de ordening omkeren, zijn het anti-isomorfismen op.

Bijgevolg kan een Galoisuitbreiding L van K met $|L:K| < \infty$ maar eindig veel tussenlichamen hebben, omdat $G_{L/K}$ slechts eindig veel ondergroepen heeft.

$G_{L/K}$ kan men als volgt beschrijven. Is L Galoisuitbreiding van K met $|L:K| < \infty$, dan is L splijtlichaam van een separabele veelterm f over K. Laat f in L de wortels $x_1, \ldots, x_n$ hebben. Elke $\sigma \in G$ permuteert deze wortels; aangezien $L = K(x_1, \ldots, x_n)$, is σ door z'n werking op $x_1, \ldots, x_n$ volledig bepaald. $G_{L/K}$ is dus te interpreteren als ondergroep van S_n, de groep van alle permutaties van n symbolen (i.c. $x_1, \ldots, x_n$). Een onmiddellijk gevolg is

(13.2) Stelling. Zij L een Galoisuitbreiding van K, $|L:K| < \infty$, L splijtlichaam van $f \in K[X]$ over K, $gr(f) = n$. Dan is $|G_{L/K}| \leq n!$

Twee tussenlichamen van L en K heten geconjugeerd, als de één door een element van $G_{L/K}$ op de ander wordt afgebeeld. Ga na dat dit een equivalentierelatie is. Is L een Galoisuitbreiding van K met $|L:K| < \infty$, dan corresponderen geconjugeerde tussenlichamen met geconjugeerde ondergroepen van $G_{L/K}$; zie het bewijs van (12.1), (iii).

Opgaven.

1. Zij G een eindige groep van automorfismen van het lichaam L, $K = Inv(G)$. Dan is L een Galoisuitbreiding van K met Galoisgroep G.

2. Zij kar.$K \neq 2$. We beschouwen $f(X) = aX^2 + bX + c \in K[X]$, $a \neq 0$. Definieer de discriminant D van f door $D = b^2 - 4ac$. Bewijs: f heeft een wortel in $K \Leftrightarrow D = d^2$ voor een $d \in K$ (of, zoals we meestal zeggen: $D \in K^2$).

3. Beschouw $f(X) = X^3 - 2$ in $\mathbb{Q}[X]$.
(i) Bewijs dat f geen wortels heeft in $\mathbb{Q}$.
(ii) Laat zien dat f irreducibel is in $\mathbb{Q}$.
(iii) Beschouw een uitbreiding $\mathbb{Q}(\alpha)$ van $\mathbb{Q}$, waarin α een wortel is van f. N.B.: we vatten α niet op als complex getal. Het is echter nuttig deze opgave ook te maken binnen het kader van

de complexe getallen.

(iv) In $\mathbb{Q}(\alpha)[X]$ is $f(X) = (X-\alpha)g(X)$. Laat zien dat g irreducibel is in $\mathbb{Q}(\alpha)[X]$. (Aanwijzing: zie vorige opgave).

(v) Adjungeer een wortel β van g aan $\mathbb{Q}(\alpha)$. $\mathbb{Q}(\alpha,\beta)$ is een Galoisuitbreiding van $\mathbb{Q}$. Wat is $|\mathbb{Q}(\alpha,\beta) : \mathbb{Q}|$? Hoe ziet de Galoisgroep $G = G_{\mathbb{Q}(\alpha,\beta)/\mathbb{Q}}$ er dus uit?

(vi) Schrijf de elementen van G als permutaties van de wortels van f. Wat zijn de ondergroepen van G? Welke tussenlichamen van $\mathbb{Q}(\alpha,\beta)$ en $\mathbb{Q}$ vindt U op deze wijze? Welke daarvan zijn normaal over $\mathbb{Q}$?.

4. Beschouw $f(X) = X^4 - 3$ in $\mathbb{Q}[X]$.

(i) Bewijs dat f geen wortels in $\mathbb{Q}$ heeft.

(ii) Laat zien dat f geen kwadratische factoren in $\mathbb{Q}[X]$ heeft. f is dus irreducibel (waarom?) .

(iii) Zij $\alpha\,(=\sqrt[4]{3})$ een reëel getal zodat $\alpha^4 = 3$.
Wat zijn de andere wortels van f in $\mathbb{C}$?

(iv) Zij K het splijtlichaam van f in $\mathbb{C}$. Wat is $|K : \mathbb{Q}|$?
Bewijs Uw bewering terdege!

(v) Beschrijf de elementen van $G = G_{K/\mathbb{Q}}$ als permutaties van de wortels van f. Aanwijzing: ga na hoe $\sigma \in G$ op α en op i moet werken!

(vi) Schrijf de elementen van G die U in (v) gevonden hebt, onder elkaar met achter elk element z'n orde. Bepaal alle cyclische ondergroepen van G en vervolgens alle niet-cyclische ondergroepen. U moet in totaal 10 ondergroepen vinden, $\langle 1 \rangle$ en G zelf meegerekend.

(vii) Bepaal de tussenlichamen van K en $\mathbb{Q}$. Welke daarvan zijn normaal over $\mathbb{Q}$? Welke tussenlichamen zijn geconjugeerd met elkaar?

14. **Zij** L een separabele uitbreiding van K van eindige graad : $|L : K| = n$. Neem voor M een willekeurige uitbreiding van L die een Galoisuitbreiding van K is. Laat $\sigma_1, \ldots, \sigma_n$ de verschillende K-isomorfismen van L in M zijn. Dan definiëren we voor $x \in L$:

$Sp_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$, het <u>spoor</u> van x in L/K ;

$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$, de <u>norm</u> van x in L/K .

We beweren dat spoor en norm niet van de keuze van M afhangen. Om dit in te zien, beschouwen we het minimumpolynoom f van

x over K.

$$f(X) = X^t + a_{t-1} X^{t-1} + \dots + a_1 X + a_0 .$$

Iedere $\sigma_i(x)$ is een wortel van f. Is omgekeerd y een wortel van f in M, dan is het K-isomorfisme van K(x) op K(y) voort te zetten tot een K-isomorfisme van L in M, dus tot één van de σ_i.
Bekijk de veelterm

$$g(X) = \prod_{i=1}^{n} (X - \sigma_i(x)) .$$
$$= X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0 .$$

Hierin is $b_{n-i} = (-1)^i \sum_{j_1<j_2<\dots<j_i} \sigma_{j_1}(x)\, \sigma_{j_2}(x) \dots \sigma_{j_i}(x)$.

Voor elke $\sigma \in G_{M/K}$ zijn $\sigma\sigma_1, \dots, \sigma\sigma_n$ n verschillende K-isomorfismen van L in M, dus vormen een permutatie van $\sigma_1, \dots, \sigma_n$.
Daaruit volgt $\sigma(b_{n-i}) = b_{n-i}$. Dus $b_{n-i} \in K$ voor alle i.

$$g(X) = f(X)^s h(X)$$

met $h \in K[X]$, ggd(f,h) = 1. Een wortel van h is wortel van g, dus één van de $\sigma_i(x)$, die f als minimumpolynoom hebben. Maar (f,h) = 1 , dus moet h=1 zijn. Dus $g(X) = f(X)^s$; $s = |L : K(x)|$.

$$Sp_{L/K}(x) = \sum_i \sigma_i(x) = -b_{n-1} = -s\, a_{n-1} .$$

$$N_{L/K}(x) = \prod_i \sigma_i(x) = (-1)^n b_0 = (-1)^n a_0^s .$$

Daaruit volgt dat spoor en norm van $x \in L$ niet afhangen van M.
We zien tevens dat $Sp_{L/K}(x)$ en $N_{L/K}(x) \in K$.
Voor $x \in K$ is $Sp_{L/K}(x) = nx$, $N_{L/K}(x) = x^n$.
Uit de definities volgt onmiddellijk

$$Sp_{L/K}(x+y) = Sp_{L/K}(x) + Sp_{L/K}(y)$$
$$N_{L/K}(xy) = N_{L/K}(x)\, N_{L/K}(y) .$$

(14.1) <u>Stelling</u>. Stel $K \subseteq L \subseteq M$, M separabel over K, $|M : K| < \infty$.
Dan is voor $x \in M$:

$$Sp_{M/K}(x) = Sp_{L/K} (Sp_{M/L}(x))$$

en

$$N_{M/K}(x) = N_{L/K} (N_{M/L}(x)) .$$

<u>Bewijs.</u> Neem een Galoisuitbreiding N van K die M omvat. Stel $\sigma_1, \dots, \sigma_s$ zijn de verschillende K-isomorfismen van L in N , $\tau_1, \dots, \tau_t$ de verschillende L-isomorfismen van M in N.

$\sigma_1,\ldots,\sigma_s$ zijn voort te zetten tot K-isomorfismen $\sigma'_1,\ldots,\sigma'_s$ van M in N. Dan zijn de $\sigma'_i\,\tau_j$, $1\leq i\leq r$, $1\leq j\leq s$, verschillende K-isomorfismen van M in N. Daar ze $rs = |M:K|$ in getal zijn, zijn 't precies alle K-isomorfismen van M in N. Nu is

$$\begin{aligned} Sp_{M/K}(x) &= \sum_{i,j} \sigma'_j\,\tau_j(x) \\ &= \sum_i \sigma'_i\,\Big(\sum_j \tau_j(x)\Big) \\ &= Sp_{L/K}\,\big(Sp_{M/L}(x)\big)\,. \end{aligned}$$

Analoog voor $N_{M/K}$ met Π i.p.v. Σ.

(14.2) Stelling. L separabele uitbreiding van K, $|L:K|<\infty$. Dan is er een $x\in L$ met $Sp_{L/K}(x)\neq 0$.

Bewijs. Stel voor elke $x\in L$ was $Sp_{L/K}(x)=0$. Is M een Galois-uitbreiding van K die L omvat en zijn $\sigma_1,\ldots,\sigma_n$ de verschillende K-isomorfismen van L in M, dan zou

$$\sum_i \sigma_i(x) = 0 \quad \text{voor alle } x\in L.$$

Dit betekent dat $\sigma_1,\ldots,\sigma_n$ lineair afhankelijk zijn, in strijd met de stelling van Dedekind (10.6).

Voor het navolgende hebben we een hulpstelling nodig, die we eerst bewijzen.

(14.3) Lemma. Zij K een oneindig lichaam, $f\in K[X_1,\ldots,X_n]$ zodat $f(x_1,\ldots,x_n)=0$ voor alle $x_1,\ldots,x_n\in K$. Dan is $f=0$.

Bewijs. Inductie naar n. Is n=1, dan kan $f\neq 0$ hoogstens eindig veel nulpunten hebben. Wegens $|K|=\infty$ impliceert $f(x_1)=0$ voor alle $x_1\in K$ dus f=0.

Stel $n>1$ en de stelling is bewezen voor n-1 variabelen.

$f\in K[X_1,\ldots,X_n]$ kunnen we schrijven als

$$f(X_1,\ldots,X_n) = \sum_i X_1^i f_i(X_2,\ldots,X_n)$$

met $f_i\in K[X_2,\ldots,X_n]$.

Voor alle $x_2,\ldots,x_n\in K$ is $f(X_1,x_2,\ldots,x_n)\in K[X_1]$.

$$f(X_1,x_2,\ldots,x_n) = \sum_i X_1^i f_i(x_2,\ldots,x_n)\,.$$

$f(x_1,x_2,\ldots,x_n)=0$ voor alle $x_1\in K$, dus $f(X_1,x_2,\ldots,x_n) = 0$.

Daaruit volgt dat $f_i(x_2,\dots,x_n)=0$ voor alle $x_2,\dots,x_n$, dus $f_i=0$. Dit impliceert $f=0$.

Automorfismen $\sigma_1,\dots,\sigma_n$ van een lichaam L heten algebraïsch afhankelijk over L , als er een $f\in L[X_1,\dots,X_n]$, $f\neq 0$, bestaat zodat $f(\sigma_1(x),\dots,\sigma_n(x))=0$ voor alle $x\in L$. Zijn $\sigma_1,\dots,\sigma_n$ niet algebraïsch afhankelijk over L, dan noemen we ze algebraïsch onafhankelijk over L.

(14.4) Stelling. Zij K een lichaam met oneindig veel elementen, L een Galoisuitbreiding van K met $|L:K|=n$. Dan zijn de $\sigma_1,\dots,\sigma_n\in G_{L/K}$ algebraïsch onafhankelijk over L.

Bewijs. Stel $f\in K[X_1,\dots,X_n]$ zodat $f(\sigma_1(x),\dots,\sigma_n(x))=0$ voor alle $x\in K$. Neem een basis $a_1,\dots,a_n$ van L over K.
Is $x\in L$, dan

$$x=\sum_{j=1}^{n}\xi_j a_j \quad \text{met} \quad \xi_j\in K .$$

$$\sigma_i(x) = \sum_{j=1}^{n}\xi_j\sigma_i(a_j) .$$

Volgens (12.4) is $\det(\sigma_i(a_j))\neq 0$. Zij

$$(\beta_{ij})_{i,j} = (\sigma_i(a_j))_{i,j}^{-1} .$$

Neem $Y_i = \sum_{j=1}^{n}\beta_{ij}X_j$, dan $X_i = \sum_{j=1}^{n}\sigma_i(a_j)Y_j$.

Neem $g(Y_1,\dots,Y_n)=f(X_1,\dots,X_n)$. Dan is $g(\xi_1,\dots,\xi_n) = f(\sigma_1(x),\dots,\sigma_n(x)) = 0$ voor alle $\xi_1,\dots,\xi_n$, dus $g=0$. Maar dan is ook $f=0$.

De bewijzen van (14.3) en (14.4) gebruiken dat $|K|=\infty$. Als $|K|<\infty$, dan zijn (14.3) en (14.4) allebei onjuist; zie opgaven 1 en 3.

Zij L een Galoisuitbreiding van K, $|L:K|=n$. Is $a\in L$ een element zodat $\sigma_1(a),\dots,\sigma_n(a)$ met $\sigma_i\in G_{L/K}$ K-lineair onafhankelijk zijn, dan heet $\sigma_1(a),\dots,\sigma_n(a)$ een normale basis van L over K. Iedere Galoisuitbreiding van eindige graad heeft een normale basis. We bewijzen dit hier onder de veronderstelling dat $|K|=\infty$; bij de behandeling van de eindige lichamen zullen we 't ook voor dat geval aantonen.

(14.5) <u>Stelling</u>. Zij K een oneindig lichaam, L een Galoisuitbreiding van K met $|L:K| = n$. Dan heeft L een normale basis over K.

<u>Bewijs.</u> We voeren 't bewijs in twee stappen.

(i) Als $a \in L$ zodat $\det(\sigma_i\sigma_j(a)) \neq 0$, dan is $\sigma_1(a), \ldots, \sigma_n(a)$ een normale basis.

(ii) Er is een $a \in L$ zodat $\det(\sigma_i\sigma_j(a)) \neq 0$.

Ad (i). Stel $\lambda_j \in K$ zodat $\sum_j \lambda_j\sigma_j(a) = 0$.

Voor elke i is dan $\sum_j \lambda_j\sigma_i\sigma_j(a) = \sigma_i(\sum_j \lambda_j\sigma_j(a)) = 0$.

Wegens $\det(\sigma_i\sigma_j(a)) \neq 0$ impliceert dit $\lambda_1 = \ldots = \lambda_n = 0$.

Opmerking: bewijs zelf het omgekeerde van (i). Merk op dat we tot nu toe niet gebruikt hebben dat $|K| = \infty$.

Ad (ii). $\sigma_1, \ldots, \sigma_n$ vormen een groep, n.l. $G_{L/K}$. Dus $\sigma_i\sigma_j = \sigma_{k(i,j)}$. Bekijk de veelterm

$$f(X_1, \ldots, X_n) = \det(X_{k(i,j)}) .$$

Dan is

$$f(\sigma_1(a), \ldots, \sigma_n(a)) = \det(\sigma_i\sigma_j(a)) .$$

Als we aantonen dat $f \neq 0$, dan is er dus een a zodat $\det(\sigma_i\sigma_j(a)) \neq 0$. Vervang in de matrix $(X_{k(i,j)})_{i,j}$ X_1 door 1, $X_2, \ldots, X_n$ door 0. In iedere rij en in iedere kolom staat er dan precies één 1 en verder overal 0, dus de determinant van deze matrix is ± 1. Dus $f(1,0,\ldots,0) = \pm 1 \neq 0$, derhalve $f \neq 0$.

<u>Opgaven</u>.

1. Zij K een eindig lichaam, $|K| = q$. $h \in K[X]$ definiëren we door $h(X) = X^q - X$. Laat zien dat $h(x) = 0$ voor alle $x \in K$.

2. K als in de vorige opgave. Zij $I = \{ f \in K[X] \mid f(x) = 0$ voor alle $x \in K \}$.

(i) Laat zien dat I een ideaal is in $K[X]$. Dus I is een hoofdideaal.

(ii) Bewijs dat $I = (h)$ met $h(X) = X^q - X$.

3. Zij K een lichaam met p elementen (p priem), L een kwadratische uitbreiding van K. L heeft dus p^2 elementen. Voor het bestaan van zo'n L, zie § 18 in dit dictaat.

(i) Bewijs dat $\varphi: x \to x^p$ een K-automorfisme van L is.

(ii) Laat zien dat φ niet de identiteit is.

(iii) Neem $f \in K[X_1, X_2]$ met $f(X_1, X_2) = X_1{}^p - X_2$.

Bewijs dat $f \neq 0$ en dat $f(\varphi(x), x) = 0$ voor alle $x \in L$, m.a.w.

dat φ en de identiteit algebraïsch afhankelijk zijn over L.

15. Een algebraïsche uitbreiding L van een lichaam K heet een enkelvoudige (of monogene) uitbreiding als er een $x \in L$ is zodat $K(x) = L$. x heet een primitief element van L t.o.v. K.

(15.1) Stelling. Stel $|L:K| < \infty$, $|K| = \infty$. L is dan en slechts dan een monogene uitbreiding van K als er maar eindig veel tussenlichamen van L en K zijn.

Bewijs. Stel $L = K(x)$. Zij f de minimumveelterm van x over K. Is M een tussenlichaam van K en L, dan voegen we aan M de minimumveelterm g van x over M toe. g is een deler van f. Aangezien f maar eindig veel delers heeft is het voldoende aan te tonen dat M door g bepaald is.
$g(X) = a_0 + a_1 X + \dots + a_k X^k$ met $a_i \in L$. $M' = K(a_0, a_1, \dots, a_k) \subseteq M$. g is irreducibel in $M[X]$, dus ook in $M'[X]$. Omdat $L = M(x) = M'(x)$, is $|L:M'| = k = |L:M|$. Dus $M = M'$, d.w.z. M is door g bepaald. Stel omgekeerd dat er maar eindig veel tussenlichamen van L en K zijn. $L = K(a_1, \dots, a_n)$ met $a_i \in L$. Als we kunnen bewijzen dat voor $a, b \in L$: $K(a,b) = K(c)$ voor zekere c, dan volgt daaruit met inductie dat L te schrijven is als $K(x)$. Bekijk dus $K(a,b)$. Neem $c(\lambda) = a + \lambda b$, $\lambda \in K$. Er zijn maar eindig veel lichamen tussen K en $K(a,b)$. Aangezien $|K| = \infty$, moeten er dus λ en $\mu \in K$ zijn, $\lambda \neq \mu$, zodat $K(c(\lambda)) = K(c(\mu))$.
$c(\lambda) - c(\mu) = (\lambda - \mu)b$, dus $b \in K(c(\lambda))$. Maar dan ook $a = c(\lambda) - \lambda b \in K(c(\lambda))$. Dus $K(c(\lambda)) = K(a,b)$.

(15.2) Stelling. $|K| = \infty$, $|L:K| < \infty$, L separabel over K. Dan is L een enkelvoudige uitbreiding van K.

Bewijs. Zij M de normale afsluiting van L over K. M is een Galoisuitbreiding van K, $|M:K| < \infty$. Er zijn dus maar eindig veel lichamen tussen M en K, dus zeker tussen L en K. Volgens de vorige stelling is L dus een enkelvoudige uitbreiding van K.

Opmerking. De stellingen (15.1) en (15.2) gelden ook voor eindige lichamen K zoals we later zullen zien.

Opgaven.

1. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(i) Bepaal $|L:\mathbb{Q}|$.
(ii) Toon aan dat L een monogene uitbreiding is van $\mathbb{Q}$.

(iii) Bepaal een x zodat $L = \mathbb{Q}(x)$.

(iv) Wat is de minimumveelterm f over $\mathbb{Q}$ van de x die U in (iii) gevonden hebt? Bepaal de andere wortels van f.

(v) Bewijs dat L normaal is over $\mathbb{Q}$.

(vi) Bepaal de Galoisgroep van L over $\mathbb{Q}$.

(vii) Bepaal de tussenlichamen van L en $\mathbb{Q}$. Welke daarvan zijn normaal over $\mathbb{Q}$?

16. Onder een <u>gerichte verzameling</u> verstaan we een geordende verzameling V met de volgende eigenschap : voor elke α en β in V is er een $\gamma \in V$ zodat $\gamma \geq \alpha, \geq \beta$.

Zij I een gerichte verzameling. Een <u>projectief systeem</u> $(X_\alpha, \pi_\beta^\alpha)$ over I is een collectie verzamelingen X_α, $\alpha \in I$, met afbeeldingen $\pi_\beta^\alpha : X_\alpha \to X_\beta$ voor $\alpha \geq \beta$, die aan de volgende eisen voldoen:

(i) $\pi_\alpha^\alpha = 1_\alpha$, de identiteit op X_α, voor alle $\alpha \in I$;

(ii) voor $\alpha \geq \beta \geq \gamma$ is $\pi_\gamma^\alpha = \pi_\gamma^\beta \circ \pi_\beta^\alpha$

Een <u>projectief systeem van groepen</u> $(G_\alpha, \pi_\beta^\alpha)$ is een projectief systeem, waarin de G_α groepen zijn en de π_β^α groepshomomorfismen. Analoog bestaat een <u>projectief systeem van topologische ruimten</u> $(X_\alpha, \pi_\beta^\alpha)$ uit topologische ruimten X_α en continue afbeeldingen π_β^α, van <u>topologische groepen</u> $(G_\alpha, \pi_\beta^\alpha)$ uit topologische groepen G_α en continue homomorfismen π_β^α.

Is J een gerichte deelverzameling van I en $(X_\alpha, \pi_\beta^\alpha)$ een projectief systeem over I, dan heet $(X_\alpha, \pi_\beta^\alpha)_J$, bestaande uit de X_α en de π_β^α met α en $\beta \in J$, een <u>deelsysteem</u> van $(X_\alpha, \pi_\beta^\alpha)$. J heet <u>cofinaal</u> in I, als er bij elke $\alpha \in I$ een $\beta \in J$ bestaat met $\beta \geq \alpha$. Is J cofinaal in I, dan heet $(X_\alpha, \pi_\beta^\alpha)_J$ een <u>cofinaal deelsysteem</u> van $(X_\alpha, \pi_\beta^\alpha)$.

Zij $(X_\alpha, \pi_\beta^\alpha)$ en projectief systeem over I. De <u>projectieve limiet</u> $\varprojlim_I (X_\alpha, \pi_\beta^\alpha)$, of kortweg $\varprojlim X_\alpha$, definiëren we door

$$X_\infty = \varprojlim X_\alpha = \{(x_\alpha) \in \prod_{\alpha \in I} X_\alpha \mid \text{voor } \alpha \geq \beta \text{ is } \pi_\beta^\alpha X_\alpha = X_\beta\} .$$

$\pi_\alpha : X_\infty \to X_\alpha$ wordt gedefinieerd door $\pi_\alpha((x_\gamma)) = x_\alpha$.
Ga na, dat voor $\alpha \geq \beta$: $\pi_\beta^\alpha \circ \pi_\alpha = \pi_\beta$.

Is $(G_\alpha, \pi_\beta^\alpha)$ een projectief systeem van groepen, dan kunnen

we $G_\infty = \varprojlim G_\alpha$ als volgt van een groepsstructuur voorzien:

$$(x_\alpha)\cdot(y_\alpha) = (x_\alpha \cdot y_\alpha) .$$

Eenheidselement is (e_α), met e_α 't eenheidselement van G_α. $(x_\alpha)^{-1} = (x_\alpha^{-1})$. Ga na dat aan alle axioma's voor een groep voldaan is. Met $\varprojlim G_\alpha$ bedoelen we in dit geval altijd de aldus gedfinieerde <u>groep</u>. Ga na, dat de π_α homomorfismen zijn in dit geval.

Is $(X_\alpha, \pi_\beta^\alpha)$ een projectief systeem van topologische ruimten, dan maken we van $X_\infty = \varprojlim X_\alpha$ een topologische ruimte door de definitie: een basis van de open verzamelingen in X_∞ wordt gevormd door de verzamelingen $\pi_\alpha^{-1}(O_\alpha)$, O_α open in X_α, $\alpha \in I$. Ga zelf na dat dit een goede basis is, d.w.z. : X_∞ is **vereniging** van basisverzamelingen; de doorsnede van twee basisverzamelingen is er weer één. De π_α zijn continu.

De projectieve limiet van een systeem van topologische groepen is weer een topologische groep, zoals we inzien door de bovenstaande beschouwingen over groepen en topologische ruimten te combineren.

We beschouwen nu een projectief systeem $(X_\alpha, \pi_\beta^\alpha)$ over I en een cofinaal deelsysteem $(X_\alpha, \pi_\beta^\alpha)_J$. We willen aantonen dat er een 1-1 afbeelding φ van $\varprojlim_I X_\alpha$ op $\varprojlim_J X_\alpha$ bestaat. Definieer de afbeelding φ door

$$\varphi((x_\alpha)_{\alpha \in I}) = (x_\alpha)_{\alpha \in J} .$$

Ga na dat φ een afbeelding van $\varprojlim_I X_\alpha$ in $\varprojlim_J X_\alpha$ is. We definiëren nu een afbeelding ψ in omgekeerde richting op de volgende manier :

$$\psi((x_\alpha)_{\alpha \in J}) = (y_\beta)_{\beta \in I} ,$$

waarin y_β gedefinieerd is door :

$$\text{voor } \alpha \in J ,\ \alpha \geq \beta, \quad \text{is} \quad y_\beta = \pi_\beta^\alpha\, x_\alpha .$$

Omdat J cofinaal is in I, is er minstens één zo'n α. Ga zelf na dat voor $\alpha_1 \geq \beta$ en $\alpha_2 \geq \beta$ moet gelden :

$$\pi_\beta^{\alpha_1} x_{\alpha_1} = \pi_\beta^{\alpha_2} x_{\alpha_2} .$$

Men verifieert zonder veel moeite dat $\varphi \circ \psi = 1$ en $\psi \circ \varphi = 1$. Dus φ heeft een inverse, n.l. ψ, en is derhalve 1-1 en op.

Is $(X_\alpha, \pi_\beta^\alpha)$ een projectief systeem van groepen, topologische ruimten of topologische groepen, dan is de boven gedefinieerde afbeelding φ een isomorfisme, homeomorfisme resp. continu isomorfisme. Ga dit zelf na!

<u>Opgave</u>.

1. Zij G een groep, I de verzameling van alle normaaldelers van G.
Voor H_1 en $H_2 \in I$ definiëren we $H_1 \leq H_2$ als $H_1 \supseteq H_2$. Toon aan dat I een gerichte verzameling is. Voor $H \in I$ is $G_H = G/H$. Voor $H_1 \geq H_2$ is $\pi_{H_2}^{H_1}$ het natuurlijke homomorfisme van G/H_1 op $G/H_2 \cong G/H_1 \big/ H_2/H_1$. Laat zien dat we op deze wijze een projectief systeem hebben verkregen.
Zij $G_\infty = \varprojlim_I G_H$. Laat zien dat

$$\varphi : g \to (gH)_{H \in I}$$

een homomorfisme is van G in G_∞. Bewijs dat φ een isomorfisme op is.

17. We bekijken nu een Galoisuitbreiding L van een lichaam K met $|L : K| = \infty$. $G_{L/K}$ is dan een oneindige groep.
Zij I de verzameling van alle tussenlichamen M van L en K met $|M : K| < \infty$, die een Galoisuitbreiding van K zijn. Voor dit laaste is voldoende dat M normaal is over K. I wordt geordend door inclusie, d.w.z. voor $M, N \in I$ is $M \leq N$ als $M \subseteq N$. I is een gericht systeem. Voor $M, N \in I$ is n.l. MN een normale uitbreiding van K met $|MN : K| < \infty$, dus $MN \in I$ en $MN \geq M, \geq N$.
Voor $M \in I$ definiëren we $G_M = G_{M/K}$. Voor $M \geq N$ nemen we voor π_N^M de afbeelding die aan $\sigma \in G_{M/K}$ z'n restrictie tot N toevoegt.
Ga na dat π_N^M een homomorfisme van G_M op G_N is. $(G_M, \pi_N^M)_{M,N \in I}$ is een projectief systeem van topologische groepen, als we de eindige groepen G_M van de discrete topologie voorzien. We definiëren de topologische groep G_∞ door $G_\infty = \varprojlim G_M$.
We zullen nu eerst aantonen dat $G_{L/K}$ als abstracte groep isomorf is met G_∞.
Definieer φ door

$$\varphi(\sigma) = (\sigma|M)_{M \in I} \quad \text{voor } \sigma \in G_{L/K}.$$

φ is een homomorfisme van $G_{L/K}$ in G_∞. We laten nu zien dat φ zelfs een isomorfisme op is.

(i) φ is 1-1. Stel $\sigma \neq 1$ in $G_{L/K}$. Dan is er een $x \in L$ zodat $\sigma(x) \neq x$. Neem voor M de normale afsluiting van K(x) in L. Dan is $\sigma|M \neq 1$ op M, dus $\varphi(\sigma) \neq 1$.

(ii) φ is op. Zij $(\sigma_M)_{M\in I} \in G_\infty$. Definieer σ als volgt:

Voor $x \in L$ nemen we voor M de normale afsluiting van K(x) in L. Dan is $\sigma(x) = \sigma_M(x)$. Voor $x \in K$ is dus $\sigma(x) = x$.

Zijn x en $y \in L$, dan is er een $N \in I$ met $x, y \in N$. Omdat $(\sigma_M)_{M\in I} \in G_\infty$, is $\sigma(x) = \sigma_N(x)$, $\sigma(y) = \sigma_N(y)$ (waarom?). Dus $\sigma(x+y) = \sigma(x)+\sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$, d.w.z. σ is een K-isomorfisme van L in zichzelf. Omdat L normaal is over K, is σ dus een K-automorfisme van L, d.w.z. $\sigma \in G_{L/K}$. Het is duidelijk dat $\varphi(\sigma) = (\sigma_M)_{M\in I}$, waarmee aangetoond is dat φ op is.

We identificeren verder $G_{L/K}$ met G_∞ via het boven gedefinieerde isomorfisme φ. Dat wil dus zeggen dat we de topologie van G_∞ op $G_{L/K}$ overbrengen door middel van φ. Samengevat:

Is L een Galoisuitbreiding van K met $|L : K| = \infty$, dan definiëren we de <u>Galoisgroep $G_{L/K}$ van L over K</u> als de <u>topologische groep</u> $\varprojlim_I G_{M/K}$, als I het gerichte systeem is van de normale uitbreidingen M van K met $|M : K| < \infty$. De elementen van $G_{L/K}$ blijven we opvatten als K-automorfismen van L.

We willen nu de topologie van $G_{L/K} = G_\infty$ aan een nader onderzoek onderwerpen.

$G_\infty = \varprojlim G_{M/K}$. $\pi_M : G_\infty \to G_{M/K}$ is niets anders dan het restrictiehomomorfisme $\sigma \to \sigma|M$. Een basis van de open verzamelingen in G_∞ wordt dus gevormd door de $\pi_M^{-1}(O)$, O open in $G_{M/K}$. Aangezien iedere deelverzameling van $G_{M/K}$ open is, vormen de $\pi_M^{-1}(\tau)$, $M \in I$, $\tau \in G_{M/K}$ een basis van de topologie in G_∞. Dit zijn precies alle verzamelingen van het type

$$O(M, \rho) = \{\sigma \in G_{L/K} \mid \sigma|M = \rho|M\}, \quad M \in I, \ \rho \in G_{L/K}.$$

Laat nu $x_1, \dots, x_n$, $y_1, \dots, y_n$ elementen zijn van L. Bekijk de verzameling

$$O(x_1, \dots, x_n; y_1, \dots, y_n) = \{\sigma \in G_{L/K} \mid \sigma(x_i) = y_i, \ i = 1, \dots, n\}.$$

We beweren dat $O(x_1, \dots, x_n; y_1, \dots, y_n)$ open is. Is n.l. $O(x_1, \dots, x_n; y_1, \dots, y_n) \neq \emptyset$, dan is er een $\rho \in G_{L/K}$ zodat

$\rho(x_i) = y_i$, $i=1,\ldots,n$. Zij M de normale afsluiting van $K(x_1,\ldots,x_n)$ in L. De restrictie van ρ tot $K(x_1,\ldots,x_n)$ kan op eindig veel manieren voortgezet worden tot een K-isomorfisme van M in L, zeg tot $\rho_1',\ldots,\rho_s'$. Iedere ρ_i' is voort te zetten tot een K-automorfisme ρ_i van L. Dan is

$$O(x_1,\ldots,x_n;\ y_1,\ldots,y_n) = O(M,\rho_1) \cup \ldots \cup O(M,\rho_s) .$$

Zij anderzijds $M \in I$. Neem een K-basis $x_1,\ldots,x_n$ van M. Dan is

$$O(M,\rho) = O(x_1,\ldots,x_n;\ \rho(x_1),\ldots,\rho(x_n)) .$$

Men gaat gemakkelijk na dat de $O(x_1,\ldots,x_n;\ y_1,\ldots,y_n)$ een basis van de open verzamelingen in $G_{L/K}$ vormen. Daarmee hebben we een beschrijving van de topologie in $G_{L/K}$ die de projectieve limiet en de normale tussenlichamen M met $|M:K| < \infty$ niet nodig heeft.

We beschouwen nu een willekeurig tussenlichaam M van K en L. $G_{L/M}$ is een ondergroep van $G_{L/K}$. We beweren dat $G_{L/M}$ gesloten is.
Stel n.l. $\sigma \in G_{L/K}$, $\sigma \notin G_{L/M}$. Dan is er een $x \in M$ zodat $\sigma(x) \neq x$. $O(x;\ \sigma(x))$ is dan een omgeving van σ met $O(x;\ \sigma(x)) \cap G_{L/M} = \emptyset$.
Bij de formulering van een hoofdstelling van de Galoistheorie voor 't geval $|L:K| = \infty$ zullen we dus met gesloten ondergroepen van G moeten werken.
Met $\underline{\underline{G}}$ of $\underline{\underline{G}}_{L/K}$ noteren we de tralie van de gesloten ondergroepen van $G_{L/K}$, geordend door inclusie, met $\underline{\underline{L/K}}$ de tralie van de tussenlichamen M van L en K, eveneens geordend door inclusie.
Dan geldt :

(17.1) Hoofdstelling van de Galoistheorie (oneindige graad). Zij L een Galoisuitbreiding van K, $|L:K| = \infty$. De afbeeldingen

$$g : \underline{\underline{L/K}} \to \underline{\underline{G}}_{L/K}$$

gedefinieerd door

$$g(M) = G_{L/M} ,$$

en

$$i : \underline{\underline{G}}_{L/K} \to \underline{\underline{L/K}}$$

gedefinieerd door

$$i(H) = \mathrm{Inv}(H)$$

zijn anti-isomorfismen op, en wel elkaars inverse.

Bewijs. $i \circ g = 1$ volgt weer uit (10.4)(ii), net als in het bewijs van (13.1).
Zij omgekeerd H een gesloten ondergroep van $G_{L/K}$. $g \circ i(H) \supseteq H$ is duidelijk. Stel $\sigma \in g \circ i(H)$. We kunnen volstaan met aan te tonen dat iedere basisomgeving $O(x_1,\ldots,x_n;\ \sigma(x_1),\ldots,\sigma(x_n))$ van σ een element van H bevat. Immers, dan is σ verdichtingspunt van H, dus $\sigma \in H$ wegens de geslotenheid van H.
Beschouw $O(x_1,\ldots,x_n;\ \sigma(x_1),\ldots,\sigma(x_n))$. Vorm de normale afsluiting N in L van $M(x_1,\ldots,x_n)$ over M. $|N:M| < \infty$, N is een Galoisuitbreiding van M. Bekijk de groep $H' = \{\tau|N \mid \tau \in H\}$. Het is duidelijk dat $H' \subseteq G_{N/M}$, want $M = Inv(H)$. Uit $M = Inv(H)$ volgt anderzijds dat M het invariantielichaam in N van H' is, dus moet $H' = G_{N/M}$. Nu is $\sigma \in G_{L/M}$. Omdat N normaal is over M, is $\sigma(N) = N$. Dus $\sigma|N \in G_{N/M} = H'$, dus er is een $\tau \in H$ met $\tau|N = \sigma|N$, d.w.z. $\tau \in O(N,\sigma) \subseteq O(x_1,\ldots,x_n,\ \sigma(x_1),\ldots,\sigma(x_n))$. Daarmee is aangetoond dat $g \circ i = 1$. De rest van het bewijs loopt net als bij (13.1) en wordt derhalve aan de lezer overgelaten.

We besluiten deze paragraaf met op te merken dat de Galoistheorie van eindig dimensionale Galoisuitbreidingen in feite ook onder bovenstaande theorie valt. De topologie van de Galoisgroep is in dat geval n.l. de discrete topologie, dus iedere ondergroep van de Galoisgroep is gesloten (en open).

Opgaven.

* 1. Zij L een Galoisuitbreiding van K, G de topologische Galoisgroep van L over K.
Zij voor $x \in L$, V_x de verzameling van geconjugeerden van x in L.

We voorzien V_x van de discrete topologie; aangezien V_x eindig is, is V_x compact.

Zij $V = \prod_{x \in L} V_x$, voorzien van de Tychonow-topologie. V is dus compact volgens de stelling van Tychonow.
Definieer $\varphi : G \to V$ door
$$\varphi(g) = (g(x))_{x \in L}$$
Bewijs achtereenvolgens :
(i) φ is 1-1 ,
(ii) φ is een homeomorfisme van G op $\varphi(G)$, opgevat als topologische deelruimte van V.

(iii) $\varphi(G)$ is gesloten in V.
(iv) G is compact.

2. Zij L een Galoisuitbreiding van K, $|L:K| = \infty$. We willen aantonen dat de Galoisgroep $G_{L/K}$ minstens de machtigheid van het continuum heeft (zie ook de opmerking aan 't eind van het bewijs van (12.3)).
(i) Bewijs dat er een rij tussenlichamen van K en L bestaat: $K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n \subset K_{n+1} \subset \ldots \subset L$ met de volgende eigenschappen: $K_{n+1} \neq K_n$, K_n normaal over K, $|K_n : K| < \infty$, voor alle n.
Noem $|K_n : K_{n-1}| = r_n$ (dus $r_n > 1$), $M = \bigcup_n K_n$.
(ii) Laat zien dat M een Galoisuitbreiding is van K.
(iii) Bewijs dat $|G_{L/K}| \geq |G_{M/K}|$.
De elementen van $G_{K_1/K}$ worden nu op een willekeurige manier genummerd : $1, 2, \ldots, r_1$. De voortzettingen tot K_2 van het element van $G_{K_1/K}$ met nummer a_1 duiden we aan met $a_1 1, a_1 2, \ldots, a_1 r_2$. Zo gaan we met de inductie verder : heeft $\sigma \in G_{K_n/K}$ het nummer $a_1 a_2 \ldots a_n$; dan krijgen zijn voortzettingen tot K_{n+1} (in willekeurige volgorde) de "nummers" $a_1 a_2 \ldots a_n 1$, $a_1 a_2 \ldots a_n 2, \ldots$ $\ldots, a_1 a_2 \ldots a_n r_{n+1}$.
φ definiëren we nu als volgt:
Is $\sigma \in G_{M/K}$, dan $\varphi(\sigma) = a_1 a_2 \ldots a_n \ldots\ldots$, waarbij deze oneindige rij natuurlijke getallen gedefinieerd is door

$$a_1 \ldots a_n = \text{rangnummer van } \sigma|K_n .$$

(iv) Bewijs dat φ een 1-1 afbeelding op is van G op de oneindige rijtjes natuurlijke getallen

$$a_1 a_2 \ldots a_n a_{n+1} \ldots\ldots$$

met $\quad 1 \leq a_n \leq r_n \quad$ voor alle n.
(v) Bewijs dat $G_{M/K}$ de machtigheid van het continuum heeft.
Met (iii) samen geeft dit het aangekondigde resultaat over $G_{L/K}$.

3. Zij L een Galoisuitbreiding van K met $|L:K| = \infty$, H een willekeurige ondergroep van de Galoisgroep $G_{L/K}$, M het invariantielichaam van H. Bewijs : de Galoisgroep $G_{L/M}$, opgevat als ondergroep van $G_{L/K}$, is de afsluiting van H in de topologie van $G_{L/K}$.

4. Zij $\mathbb{F}_p$ 't lichaam met p elementen, $\bar{\mathbb{F}}_p$ z'n algebraïsche afsluiting. σ is het $\mathbb{F}_p$ -automorfisme van $\bar{\mathbb{F}}_p$ met $\sigma(x) = x^p$. Bewijs dat σ oneindige orde heeft in $G_{\bar{\mathbb{F}}_p/\mathbb{F}_p}$. [Opmerking : algemeen geldt zelfs voor eindige lichamen K dat ieder element $\neq 1$ van $G_{\bar{K}/K}$ oneindige orde heeft! We komen hier later op terug.]
Toon aan dat de door σ voortgebrachte ondergroep van $G_{\bar{\mathbb{F}}_p/\mathbb{F}_p}$ niet gesloten is. [Aanwijzing : bepaal het invariantielichaam van σ; gebruik opgaven 2 en 3.]

5. Zij n een vast natuurlijk getal, K een lichaam van karakteristiek 0, dat alle n-de eenheidswortels bevat.
$L = K(T_1, T_2, \ldots, T_i, \ldots)$, waarin $T_1, T_2, \ldots, T_i \ldots$ een (oneindig) stel algebraïsch onafhankelijke elementen zijn.
$L_i = K(\sqrt[n]{T_1}, \sqrt[n]{T_2}, \ldots, \sqrt[n]{T_i}, T_{i+1}, T_{i+2}, \ldots)$ voor $i=1,2,\ldots$. $M = \bigcup_{i=1}^{\infty} L_i$.
Bewijs :
(i) $|L_i : L_{i-1}| = n$.
(ii) M is normaal en separabel over L.
(iii) Als $\sigma \in G_{M/L}$, dan $\sigma^n = 1$. [Aanwijzing : bekijk de werking van σ op iedere $\sqrt[n]{T_i}$ afzonderlijk.]

=============

Hoofdstuk IV. Toepassingen van de Galoistheorie.

18. Eindige lichamen.

Een element x van een lichaam K heet een n-de eenheidswortel, als $x^n = 1$.
In het lichaam van de complexe getallen bijvoorbeeld zijn de n-de eenheidswortels de getallen
$e^{\frac{2\pi ik}{n}}$, $k = 0,1,2,\ldots,n-1$. Deze vormen een cyclische groep van orde n. Algemeen geldt iets dergelijks, zoals we zullen laten zien.

(18.1) Hulpstelling. Zij G een eindige commutatieve groep. Heeft $g \in G$ de orde r, $h \in G$ de orde s, dan is er een element in G met orde $= \mathrm{kgv}(r,s)$.
Bewijs. (a) Stel eerst $\mathrm{ggd}(r,s) = 1$. Dan is $\mathrm{kgv}(r,s) = rs$.

Duidelijk is dat $(gh)^{rs} = 1$. Stel ongekeerd $(gh)^k = 1$, dan $g^k h^k = 1$, dus $1 = g^{ks}h^{ks} = g^{ks}$. Dus r deelt ks, dus k. Evenzo is s een deler van k, dus ook rs. Dus de orde van gh is rs.

(b) Heeft $x \in G$ de orde r en is $d|r$, dan heeft $x^{\frac{r}{d}}$ de orde d.

(c) Zij algemeen $r = \Pi p_i^{\alpha_i}$ en $s = \Pi p_i^{\beta_i}$. Dan is

$\text{kgv}(r,s) = \Pi p_i^{\gamma_i}$ met $\gamma_i = \max(\alpha_i, \beta_i)$. Uit (b) volgt het bestaan van een element met orde $p_i^{\gamma_i}$ want $p_i^{\gamma_i}$ deelt r of s. Daar dit voor iedere i zo is, volgt uit (a) het bestaan van een element met orde $\Pi p_i^{\gamma_i}$.

(18.2) Stelling. Zij K^* de vermenigvuldigingsgroep van een commutatief lichaam K. Dan is iedere eindige ondergroep G van K^* cyclisch.

Bewijs. Stel $|G| = n$. Zij g een element met maximale orde r in G; dus $r \leq n$. Is $h \in G$, orde $h = s$, dan is er volgens (18.1) een element van G met orde $= \text{kgv}(r,s)$; omdat r maximaal was, volgt hieruit $s|r$. Dus $h^r = 1$. Dus iedere $h \in G$ is wortel van het polynoom $X^r - 1$ in K. Dus $n \leq r$. Bij elkaar geeft dit $r = n$, d.w.z. g brengt de hele groep G voort.

(18.3) Stelling. De n-de eenheidswortels in een lichaam K vormen een cyclische ondergroep van K^* met orde die n deelt.

Bewijs. Uit $x^n = y^n = 1$ volgt $(xy)^n = x^n y^n = 1$, $(x^{-1})^n = x^{-n} = 1$. Dus vormen de n-de eenheidswortels een groep, die volgens (18.2) cyclisch is. Is z een voortbrengende van deze groep, dan $z^n = 1$, dus $|G| = \text{orde } z$ is een deler van n.

We kunnen nu de structuur van eindige lichamen bepalen.

(18.4) Stelling. (i) Is K een eindig lichaam, dan $|K| = p^n$, waarin $p = \text{kar}(K)$.

(ii) Is p een priemgetal en n een natuurlijk getal, dan is er op isomorfie na precies één lichaam K met $|K| = p^n$.

Notatie: $\mathbb{F}_q$, waarin $q = p^n$.

(iii) $\mathbb{F}_q$ bestaat uit een volledig stel wortels van $X^q - X \in \mathbb{F}_p[X]$.

(iv) De elementen $\neq 0$ van $\mathbb{F}_q$ vormen een cyclische groep van orde $q-1$, d.w.z. van alle $(q-1)$-ste eenheidswortels in $\mathbb{F}_q$.

Bewijs. (i) Omdat K eindig is, is $kar(K) = p \neq 0$. K bevat het priemlichaam $\mathbb{F}_p \cong \mathbb{Z}/(p)$. K is een lineaire ruimte over $\mathbb{F}_p$ van eindige dimensie, zeg n. Zij $x_1,\ldots,x_n$ een $\mathbb{F}_p$-basis van K, dan is ieder element van K op precies één manier te schrijven als $\xi_1 x_1+\ldots+\xi_n x_n$, $\xi_i \in \mathbb{F}_p$. Voor iedere ξ_i hebben we p keuzemogelijkheden, dus in totaal zijn er p^n elementen.
(ii) en (iii). Stel $q = p^n$ en zij K een lichaam met $|K| = q$. Kar(K) is een deler van q, dus $kar(K) = p$. K bevat dus het priemlichaam $\mathbb{F}_p \cong \mathbb{Z}/(p)$. K^* is een groep met orde $q-1$, dus voor $x \in K^*$ geldt $x^{q-1} = 1$. Voor elke $x \in K$ geldt dus $x^q = x$, d.w.z. K is splijtlichaam van $X^q - X \in \mathbb{F}_p[X]$, dus op isomorfie na eenduidig bepaald. Om de existentie van een lichaam met q elementen aan te tonen nemen we het polynoom $X^q - X \in \mathbb{F}_p[X]$. Zij K een splijtlichaam van dit polynoom. Zijn x_1 en $x_2 \in K$ wortels van $X^q - X$, dan is

$$(x_1+x_2)^q = x_1^q + x_2^q = x_1 + x_2 ,$$

want $kar(K) = p$ en $q = p^n$.

$$(-x_1)^q = -x_1^q = -x_1 .$$

$$(x_1x_2)^q = x_1^q x_2^q = x_1x_2 .$$

$$(x_1^{-1})^q = (x_1^q)^{-1} = x_1^{-1} .$$

De wortels van $X^q - X$ in K vormen dus een deellichaam L van K. Omdat K als splijtlichaam minimaal is, is $K = L$. Voor $f(X)=X^q-X$ is $Df(X) = -1$, dus $(f,Df) = 1$, d.w.z. f heeft q verschillende wortels. Derhalve is $|K| = q$.
(iv) De elementen van $\mathbb{F}_q^*$ zijn de $q-1$ verschillende wortels van $X^{q-1} - 1$ in $\mathbb{F}_q$, dus vormen volgens stelling (18.3) een cyclische groep.

(18.5) Stelling. Iedere algebraïsche uitbreiding van eindige graad van een eindig lichaam is een Galoisuitbreiding. De Galoisgroep is cyclisch.

Bewijs. Beschouw het eindige lichaam $\mathbb{F}_q$ en een uitbreiding L van $\mathbb{F}_q$ met $|L : \mathbb{F}_q| = n$. Dan is $|L| = q^n$, dus $L = \mathbb{F}_{q^n}$.

L is een splijtlichaam over $\mathbb{F}_q$ van de veelterm $X^{q^n} - X$, dus is normaal en separabel. De Galoisgroep $G_{L/\mathbb{F}_q}$ heeft orde n. Het is dus voldoende aan te tonen dat er een $\mathbb{F}_q$-automorfisme van L bestaat met orde n. Beschouw σ met $\sigma(x) = x^q$. Voor $x \in \mathbb{F}_q$ is $\sigma(x) = x^q = x$. Wegens $(x_1 + x_2)^q = x_1^q + x_2^q$ en $(x_1 x_2)^q = x_1^q x_2^q$ is σ een homomorfisme, dus ook een isomorfisme, omdat L een lichaam is. Omdat L eindige orde heeft, is σ ook op. Dus is σ een $\mathbb{F}_q$-automorfisme van L.
Stel $\sigma^k = 1$ voor een natuurlijk getal k. Dan is voor alle $x \in L$, $\sigma^k(x) = x$, d.w.z. $x^{q^k} = x$, dus alle x van L zijn wortel van $X^{q^k} - X$. Dus $X^{q^n} - X \mid X^{q^k} - X$, dus $k \geq n$. Omdat anderzijds de orde van $\sigma \leq |G_{L/\mathbb{F}_q}| = n$, vinden we dat de orde van σ precies n is.

We kunnen nu de stellingen (15.1) en (15.2) over enkelvoudige uitbreidingen ook bewijzen voor eindige lichamen.

(18.6) Stelling. (15.1) en (15.2) gelden ook zonder de aanname dat $|K| = \infty$.
Bewijs. We gebruiken dezelfde notaties als in (15.1) en (15.2). We weten al dat L separabel is over K als $|K| < \infty$.
Neem een voortbrengende ζ van de cyclische groep L^*. Dan is $L = K(\zeta)$, dus monogeen. Verder is L een Galoisuitbreiding van K voor eindige K, dus hebben K en L maar eindig veel tussenlichamen.

We willen nu de stelling van de normale basis, (14.5), ook voor eindige lichamen bewijzen.

(18.7) Stelling. Is K een eindig lichaam, L een algebraïsche uitbreiding van K (dus een Galoisuitbreiding) met $|L : K| = n$, dan heeft L een normale basis over K.
Bewijs. Deze stelling volgt uit (18.5) en de nu volgende stelling, (18.8).

(18.8) Stelling. Is K een willekeurig commutatief lichaam, L een Galoisuitbreiding van K van eindige graad, zodat de Galoisgroep $G_{L/K}$ cyclisch is, dan heeft L een normale basis over K.

Bewijs. Laat σ een voortbrengende zijn van $G_{L/K}$.
Beschouw het ideaal I in K[X] van de polynomen f zodat $f(\sigma)=0$, d.w.z. $f(\sigma)(x)=0$ voor alle $x\in L$. Omdat $1,\sigma,\sigma^2,\dots,\sigma^{n-1}$ lineair onafhankelijk zijn over L volgens de stelling van Dedekind, volgt uit $f(\sigma)=0$, $f\neq 0$: $gr(f)\geq n$. Anderzijds is $\sigma^n=1$, dus voor $f(X)=X^n-1$ is $f(\sigma)=0$. Dus I is het hoofdideaal (X^n-1).
Voor $x\in L$ beschouwen we het ideaal $\{g\in K[X] \mid g(\sigma)(x)=0\}$. Dit is een hoofdideaal, zeg (g_x). Uiteraard is $g_x(X) \mid X^n-1$.
Kunnen we een x vinden met $g_x(X)=a(X^n-1)$, $a\in K^*$, dan zijn we klaar. Immers, dan zijn x, $\sigma(x)$, $\sigma^2(x),\dots,\sigma^{n-1}(x)$ K-lineair onafhankelijk, dus vormen een normale basis.
Derhalve zoeken we een x met $g_x(X)=X^n-1$.
Neem een basis $e_1,\dots,e_n$ van L over K. Stel $g_i=g_{e_i}$,

$g=\text{kgv}\{g_1,\dots,g_n\}$. Omdat $g_i|X^n-1$ voor alle i, is $g|X^n-1$.
Anderzijds is $g(\sigma)e_i=0$ voor alle i, dus $g(\sigma)x=0$ voor alle x, dus $X^n-1|g$. We mogen dus aannemen dat $g(X)=X^n-1$.
Noem de verschillende irreducibele factoren van X^n-1 in K[X] : $p_1,\dots,p_r$. Dus

$$X^n-1=p_1(X)^{n_1}\cdots\cdots p_r(X)^{n_r}.$$

Dan is $g_i(X)=p_1(X)^{k_{i,1}}\cdots\cdots p_r(X)^{k_{i,r}}$.

Voor alle j is $\max_i k_{i,j}=n_j$. Dus bij elke j is er een i_j zodat $k_{i_j,j}=n_j$.

Stel $y_j=(p_j^{-n_j}g_{i_j})(\sigma)(e_{i_j})$. Dan is $g_{y_j}=p_j^{n_j}$.

Noem nu $x=y_1+\dots+y_r$. Noem $(g_x\,p_2^{n_2}\cdots p_r^{n_r})(\sigma)=A$. Dan is $Ax=Ay_2=\dots=Ay_r=0$, dus ook $Ay_1=0$, dus

$p_1^{n_1}\mid g_x\,p_2^{n_2}\cdots p_r^{n_r}$, dus ook $p_1^{n_1}|g_x$.

Evenzo ziet men in dat $p_i^{n_i}\mid g_x$ voor alle i. Dus $X^n-1|g_x$. .

Anderzijds $g_x \mid X^n - 1$, dus op een factor uit K^* na is $g_x = X^n - 1$, waarmee het bewijs voltooid is.

Opgaven.

1. Bewijs dat ieder eindig lichaam K perfect is op de volgende twee manieren:
(i) door de afbeelding $x \to x^p$ $(p = \mathrm{kar}(K))$ te beschouwen;
(ii) door stelling (8.9) te gebruiken.

2. Zij K een eindig lichaam, L een uitbreiding van K met $|L : K| = n$. Bewijs, dat er een 1-1 correspondentie is tussen de tussenlichamen van K en L en de delers van n, en wel op twee manieren:
(i) met behulp van de hoofdstelling van de Galoistheorie;
(ii) gebruik makend van (4.1)(iii) en (18.4)(iii).

3. Bewijs dat de tralie van lichamen M tussen $\mathbb{F}_q$ en z'n algebraïsche afsluiting $\overline{\mathbb{F}}_q$ met $|M : \mathbb{F}_q| < \infty$, geordend door inclusie, isomorf is met de tralie van de natuurlijke getallen, geordend door de relatie : $d \leq n$ dan en slechts dan als $d \mid n$.

4. Beschouw een automorfisme σ van het lichaam $\mathbb{F}_q$, $q = p^d$. σ is van de gedaante $x \to x^{p^f}$, $0 \leq f < d$. Beschouw de uitbreiding $\mathbb{F}_{q^r}$ van $\mathbb{F}_q$.
(i) Bewijs dat de mogelijke voortzettingen van σ tot een automorfisme van $\mathbb{F}_{q^r}$ van de gedaante

$$\sigma_k : x \to x^{p^{f+kd}} \quad , \; 0 \leq k < r \quad ,$$

zijn.
(ii) Bewijs dat σ de orde $d/\mathrm{ggd}(f,d)$ en σ_k de orde $n/\mathrm{ggd}(f+kd,n)$ heeft, waarin $n = rd$.
(iii) Laat zien dat $r > 1$ zo gekozen kan worden dat geldt : voor alle k is de orde van $\sigma_k = r.$(orde van σ).

5. Bewijs met behulp van de vorige opgave : Is K een eindig lichaam met algebraïsche afsluiting $\overline{K}$, dan heeft iedere element $\neq 1$ van de Galoisgroep $G_{\overline{K}/K}$ oneindige orde.

19. Cirkeldeling.

Voor we ons gaan bezighouden met de n-de eenheidswortels over de rationale getallen, leiden we eerst enige hulpresultaten af.

De <u>functie van Möbius</u> μ op de natuurlijke getallen is gedefinieerd door
$\mu(1) = 1$
$\mu(n) = 0$ als n deelbaar is door een kwadraat,
$\mu(n) = (-1)^r$ als n product is van de verschillende priemgetallen $p_1, p_2, \dots, p_r$.
Ga na dat μ multiplicatief is in de zin dat $\mu(mn) = \mu(m)\mu(n)$ voor $ggd(m,n) = 1$.

(19.1) <u>Hulpstelling</u>. Zij G een (additief geschreven) commutatieve groep, f een afbeelding van de natuurlijke getallen $\mathbb{N}$ in G. $g : \mathbb{N} \to G$ zij gedefinieerd door

$$g(n) = \sum_{d|n} f(d).$$

Dan is

$$f(n) = \sum_{d|n} \mu(\tfrac{n}{d})\, g(d).$$

<u>(Omkeerformule van Möbius)</u>

<u>Bewijs</u>. We bewijzen eerst een speciaal geval, n.l. met $G = \mathbb{Z}$, de optelgroep van de gehele getallen, $f(1) = 1$, $f(n) = 0$ voor $n > 1$. Dan is dus $g(n) = 1$ voor alle n. De bewering luidt in dit geval dus

$$\mu(1) = 1 \quad , \quad \sum_{d|n} \mu(\tfrac{n}{d}) = 0 \quad \text{voor } n > 1.$$

Het laatste is equivalent met

$$\sum_{d|n} \mu(d) = 0 \quad \text{voor} \quad n > 1.$$

Schrijf $n = p_1 p_2 \dots p_r$, p_i priem (niet noodzakelijk verschillend). We passen inductie naar r toe.

$r = 1$: $\sum_{d|p_1} \mu(d) = \mu(1) + \mu(p_1) = 1 - 1 = 0.$

$r-1 \Rightarrow r$: $\sum_{d|n} \mu(d) = \sum_{d|p_1 \dots p_{r-1}} \mu(d) + \sum_{d|p_1 \dots p_{r-1}} \mu(dp_r) =$
$= 0 + 0 = 0.$

Het algemene geval bewijzen we nu als volgt.

$$\sum_{d|n} \mu(\tfrac{n}{d}) g(d) = \sum_{d|n} \mu(\tfrac{n}{d}) \sum_{e|d} f(e)$$

$$= \sum_{e|n} \Big(\sum_{e|d|n} \mu(\tfrac{n}{d}) \Big) f(e)$$

$$= f(n) \; ,$$

want $\sum_{e|d|n} \mu(\frac{n}{d}) = \sum_{\frac{n}{d}|\frac{n}{e}} \mu(\frac{n}{d}) = 0$ als $e \neq n$, 1 als $e = n$.

De <u>functie van Euler</u> φ op de natuurlijke getallen is gedefinieerd door

$\varphi(1) = 1$,
voor $n > 1$ is $\varphi(n)$ = aantal natuurlijke getallen $a < n$ met $(a,n) = 1$.

(19.2) <u>Hulpstelling</u>. Voor de functie van Euler φ geldt :
(i) $\sum_{d|n} \varphi(d) = n$.
(ii) $\varphi(n) = \sum_{d|n} \mu(\frac{n}{d})\, d$.
(iii) $\varphi(n) = n \prod_{p|n, p \text{ priem}} (1 - \frac{1}{p})$.

<u>Bewijs</u>. (i) Voor $d|n$ is $(i,n) = d \Leftrightarrow d|i$, $(\frac{i}{d}, \frac{n}{d}) = 1$.
Het aantal $i < n$ met $(i,n) = d$ is dus precies gelijk aan $\varphi(\frac{n}{d})$.
Voor iedere $i \leq n$ is er precies één $d|n$ met $(i,n) = d$.
Dus $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$.
(ii) volgt uit (i) door toepassing van de omkeerformule van Möbius.
(iii) Stel $p_1, p_2, \ldots, p_r$ zijn de verschillende priemfactoren die in n voorkomen. Uit (ii) volgt dat

$$\varphi(n) = \sum_{\varepsilon_i = 0 \text{ of } 1} \mu(p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}) \frac{n}{p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r}}$$

$$= n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) .$$

We beschouwen nu de n-de eenheidswortels over een lichaam K, d.w.z. de wortels over K van de veelterm $X^n - 1$. Zoals we gezien hebben vormen die een cyclische groep. Er zijn precies n verschillende eenheidswortels in de algebraïsche afsluiting $\overline{K}$ dan en slechts dan als $X^n - 1$ separabel is, dus als kar(K) = 0 of niet deelbaar op n. Een voortbrengende van de cyclische groep van

n-de eenheidswortels noemen we in dat geval een <u>primitieve n-de eenheidswortel</u>. Dus ζ is een primitieve n-de eenheidswortel als $\zeta^n=1$, $\zeta^k \neq 1$ voor $1 \leq k < n$. De andere n-de eenheidswortels zijn dan $\zeta^2, \zeta^3, \ldots, \zeta^{n-1}, 1$. Primitieve eenheidswortels zijn de ζ^k met $1 \leq k < n$, $(k,n) = 1$. Er zijn dus $\varphi(n)$ primitieve n-de eenheidswortels, waarin φ de functie van Euler is.

We houden ons nu verder bezig met de <u>eenheidswortels over het lichaam van de rationale getallen $\mathbb{Q}$</u>. Zij ζ een primitieve n-de eenheidswortel over $\mathbb{Q}$. Dan is

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta^i) .$$

We vormen de <u>n-de cirkeldelingsveelterm</u> Φ_n :

$$\Phi_n(X) = \prod_{(i,n)=1} (X - \zeta^i).$$

Φ_n heeft dus als wortels de primitieve n-de eenheidswortels.

(19.3) <u>Stelling</u>. (i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(ii) $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$.

<u>Bewijs.</u> (i) Zij $1 \leq i \leq n$.

$d = (i,n) \iff (\frac{i}{d}, \frac{n}{d}) = 1,\ d|n, d|i$

$\iff d|n$, ζ^i is een primitieve $\frac{n}{d}$-de eenheidswortel

$\iff d|n$, ζ^i is een wortel van $\Phi_{\frac{n}{d}}(X)$.

Dus is

$$X^n - 1 = \prod_{i=1}^{n} (X - \zeta^i)$$

$$= \prod_{d|n} \Phi_{\frac{n}{d}}(X)$$

$$= \prod_{d|n} \Phi_d(X) .$$

(ii) Neem voor G de (multiplicatief geschreven) commutatieve groep $K(x)^*$. Uit (i) en de omkeerformule van Möbius volgt direct het gestelde.

(19.4) Stelling. (i) De veeltermen Φ_n hebben gehele rationale coëfficiënten.

(ii) Iedere Φ_n is irreducibel in $\mathbb{Q}[X]$.

Bewijs. (i) Uit

$$X^n - 1 = \Phi_n(X) \cdot \prod_{d|n, d \neq n} \Phi_d(X)$$

volgt met volledige inductie naar n dat de coëfficiënten van Φ_n rationaal zijn. Schrijf

$$\Phi_d = (n_d)^{-1} \Phi^*_d \ , \quad n_d \in \mathbb{N} \ ,$$

waarin Φ^*_d een veelterm met gehele coëfficiënten is met inhoud 1, d.w.z. dat de coëfficiënten ggd 1 hebben (zie het bewijs van (2.5)). Dan is dus

$$\left(\prod_{d|n} n_d\right)(X^n - 1) = \prod_{d|n} \Phi^*_d(X) \ .$$

Het linkerlid heeft inhoud $\prod_{d|n} n_d$, het rechterlid inhoud 1. Dus moeten alle $n_d = 1$ zijn.

(ii) Zij ζ een primitieve n-de eenheidswortel, f de minimumveelterm van ζ over $\mathbb{Q}$. Dus $f \mid \Phi_n$. Is p priem met $(p,n) = 1$, dan is ζ^p ook een primitieve eenheidswortel. Zij g de minimumveelterm van ζ^p over $\mathbb{Q}$. We beweren dat g=f(op een factor na). Stel dit was niet het geval. We mogen aannemen dat f en g gehele coëfficiënten hebben en beide inhoud 1. f en g zijn irreducibel, dus $(f,g) = 1$. f en g delen Φ_n, dus ook $X^n - 1$. Dus

$$X^n - 1 = f(X)g(X)h(X).$$

Omdat f en g inhoud 1 hebben, heeft h gehele coëfficiënten. $f(\zeta) = 0$ en $g(\zeta^p) = 0$, dus ζ is een wortel van $g(X^p)$, dus $f(X) \mid g(X^p)$. Stel

$$g(X^p) = f(X) \ k(X) \ ,$$

dan heeft k ook gehele coëfficiënten.

Is $f(X) = a_t X^t + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$,

dan verstaan we onder $\bar{f} \in \mathbb{F}_p[X]$ de veelterm

$$\bar{f}(X) = \bar{a}_t X^t + \ldots + \bar{a}_1 X + \bar{a}_0$$

met $\bar{a}_i = a_i \bmod p$, als we $\mathbb{F}_p$ met $\mathbb{Z}/(p)$ identificeren.

In $\mathbb{F}_p(X)$ is $\bar{g}(X^p) = (\bar{g}(X))^p$, dus

$$(\bar{g}(X))^p = \bar{f}(X) \ \bar{k}(X).$$

$\bar{f}$ en $\bar{g}$ hebben dus een gemeenschappelijke wortel.
Wegens $(p,n) = 1$ is $X^n - 1$ separabel over $\mathbb{F}_p$. In $\mathbb{F}_p[X]$ is

$$X^n - 1 = \bar{f}(X)\,\bar{g}(X)\,\bar{h}(X) ,$$

dus $\bar{f}$ en $\bar{g}$ mogen geen gemeenschappelijke wortels hebben. Tegenspraak!
Daarmee is aangetoond: heeft de primitieve n-de eenheidswortel ζ minimumveelterm f en is p priem met $(p,n) = 1$, dan is ζ^p ook een wortel van f. Met inductie volgt hieruit dat $\zeta^{p_1 p_2 \cdots p_k}$ met p_i priem, $(p_i,n) = 1$, een wortel van f is, dus alle ζ^m met $(m,n) = 1$ zijn wortels van f. Dus $\Phi_n | f$. Daaruit volgt dat Φ_n minimumpolynoom van ζ is, dus irreducibel.

Is n geheel, dan noemen we de vermenigvuldigingsgroep van de inverteerbare elementen van $\mathbb{Z}/(n)$ de <u>restklassengroep mod n.</u>
Notatie: $(\mathbb{Z}/(n))^*$. Deze groep bestaat uit de elementen i mod n met $1 \leq i < n, (i,n) = 1$. Hij is abels, maar niet noodzakelijk cyclisch.

(19.5) <u>Stelling</u>. Zij ζ een primitieve n-de eenheidswortel over $\mathbb{Q}$.
Dan geldt:
(i) $\mathbb{Q}(\zeta)$ is een Galoisuitbreiding van $\mathbb{Q}$, $|\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(n)$.
(ii) De Galoisgroep van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorf met $(\mathbb{Z}/(n))^*$

<u>Bewijs.</u> (i) De minimumveelterm van ζ over $\mathbb{Q}$ is Φ_n, dus $|\mathbb{Q}(\zeta) : \mathbb{Q}| = gr(\Phi_n) = \varphi(n)$. Alle primitieve n-de eenheidswortels zijn machten van ζ, dus liggen in $\mathbb{Q}(\zeta)$. Dus $\mathbb{Q}(\zeta)$ is splijtlichaam van Φ_n, derhalve normaal. Wegens $kar(\mathbb{Q}) = 0$ is de uitbreiding ook separabel.
(ii) Zij G de Galoisgroep van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Voor $\sigma \in G$ is $\sigma(\zeta) = \zeta^{\alpha(\sigma)}$ met $(\alpha(\sigma),n) = 1$, want σ voert een primitieve eenheidswortel in een primitieve eenheidswortel over.

$$\alpha : \sigma \rightarrow \alpha(\sigma) \bmod n$$

is een homomorfisme van G op $(\mathbb{Z}/(n))^*$.
Maar $|G| = |\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(n) = |(\mathbb{Z}/(n))|$, dus α is een isomorfisme.

$Q(\zeta)$ als in (19.5) noemen we een <u>cirkeldelingslichaam</u>. We willen nu het geval n=p, p priemgetal $\neq 2$, aan een nader onderzoek onderwerpen. Uit (19.3)(ii) volgt

$$\Phi_p(X) = (X-1)^{-1}(X^p-1) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Zij ζ een primitieve p-de eenheidswortel, G de Galoisgroep van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. G is isomorf met $\mathbb{F}_p^*$, dus is cyclisch van de orde p-1. Zij σ een voortbrengend element van G. $\sigma(\zeta)=\zeta^{\alpha}$, $1<\alpha<p$, α mod p voortbrengende van $\mathbb{F}_p^*$.

$$\zeta^{\alpha^i}=\zeta_i \text{ , } i=0,1,\dots,p-2$$

dan is $\sigma^i(\zeta)=\zeta_i$, $\sigma\zeta_i=\zeta_{i+1}$, coëfficiënten mod p-1.

We beweren dat $\zeta_0,\zeta_1,\dots,\zeta_{p-2}$ lineair onafhankelijk zijn over $\mathbb{Q}$, dus een normale basis van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ vormen.

Stel n.l.

$$a_0\zeta_0+a_1\zeta_1+\dots+a_{p-2}\zeta_{p-2}=0$$

met rationale a_i. α mod p is een voortbrengende van $\mathbb{F}_p^*$, dus $1,\alpha,\alpha^2,\dots,\alpha^{p-2}$ mod p zijn alle elementen van $\mathbb{F}_p^*$. Daaruit volgt dat $\zeta_0,\zeta_1,\dots,\zeta_{p-2}$ een permutatie van $\zeta,\zeta^2,\dots,\zeta^{p-1}$ vormen. Dus ζ voldoet aan één vergelijking

$$\sum_{i=1}^{p-1} a_{\sigma(i)}\zeta^i=0.$$

Delen door ζ levert

$$\sum_{i=1}^{p-1} a_{\sigma(i)}\zeta^{i-1}=0.$$

Dit is een vergelijking in ζ van de graad p-2, dus van lagere graad dan Φ_p, het minimumpolynoom van ζ.

Daaruit volgt dat alle $a_{\sigma(i)}=0$, d.w.z. $a_0=\dots=a_{p-2}=0$.

Iedere $x\in\mathbb{Q}(\zeta)$ kunnen we op één manier schrijven als

$$x=\lambda_0\zeta_0+\lambda_1\zeta_1+\dots+\lambda_{p-2}\zeta_{p-2},\ \lambda_i\in\mathbb{Q}.$$

Dan is

$$\sigma^e(x)=\lambda_0\zeta_e+\lambda_1\zeta_{e+1}+\dots+\lambda_{p-2}\zeta_{p-2+e} \text{ ,}$$

coëfficiënten mod. p-1 .

$G=\langle\sigma\rangle$, dus de ondergroepen van G zijn $\langle\sigma^e\rangle$, met $ef=p-1$. Het invariantenlichaam K_e van $\langle\sigma^e\rangle$ bestaat uit de x met $\sigma^e(x)=x$.

$$x=\lambda_0\zeta_0+\dots+\lambda_{p-2}\zeta_{p-2}$$

$$\sigma^e(x)=\lambda_0\zeta_e+\dots+\lambda_{p-2}\zeta_{p-2+e}$$

Dus moet

$$\lambda_i=\lambda_{e+i}=\dots=\lambda_{(f-1)e+i} \text{ , } i=0,1,\dots,e-1 .$$

Dan is x een lineaire combinatie van de elementen

$$\eta_i = \zeta_i + \zeta_{e+i} + \dots + \zeta_{(f-1)e+i} \quad , \quad i=0,1,\dots,e-1 \quad ,$$

d.w.z. $\eta_0, \eta_1, \dots, \eta_{e-1}$ vormen een $\mathbb{Q}$-basis van het invariantenlichaam K van $\langle \sigma^e \rangle$. Iedere η_i is invariant onder $1, \sigma^e, \sigma^{2e}, \dots, \sigma^{(f-1)e}$ en onder geen enkele andere macht van σ. Dus is iedere η_i al een voortbrengende van K over $\mathbb{Q}$: $K_e = \mathbb{Q}(\eta_i)$.

Voor bijv. p=17 is $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 16$. Er zijn dus tussenlichamen K_2, K_4 en K_8 (afgezien van $\mathbb{Q}$ en $\mathbb{Q}(\zeta)$ zelf).

De Galoisgroep G van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorf met $\mathbb{F}_{17}^*$. Een voortbrengende van G is σ met $\sigma(\zeta) = \zeta^\alpha, (\alpha, 17) = 1$, α mod 17 voortbrengende van $\mathbb{F}_{17}^*$. We kunnen $\alpha = 3$ nemen; mod 17 is n.l.

$3^0=1$, $3^1=3$, $3^2=9$, $3^3=10$, $3^4=13$, $3^5=5$, $3^6=15$, $3^7=11$, $3^8=16$, $3^9=14$, $3^{10}=8$, $3^{11}=7$, $3^{12}=4$, $3^{13}=12$, $3^{14}=2$, $3^{15}=6$.

Voor $e=2$, $f=8$ krijgen we :

$$\eta_0 = \zeta_0 + \zeta_2 + \dots + \zeta_{14} = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^8 + \zeta^4 + \zeta^2 .$$

$$\eta_1 = \zeta_1 + \zeta_3 + \dots + \zeta_{15} = \zeta^3 + \zeta^{-7} + \zeta^5 + \zeta^{-6} + \zeta^{-3} + \zeta^7 + \zeta^{-5} + \zeta^6 .$$

We willen η_0 en η_1 uitrekenen.

$$\eta_0 + \eta_1 = \sum_{i=1}^{16} \zeta^i = -1 \qquad \text{(waarom?)} .$$

Uit bovenstaande uitdrukkingen voor η_0 en η_1 leidt men af :

$$\eta_0 \eta_1 = 4(\eta_0 + \eta_1) = -4 .$$

Dus η_0 en η zijn de wortels van

$$t^2 + t - 4 = 0 ,$$

dus

$$\eta_0, \eta_1 = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{17}.$$

Dus $K_2 = \mathbb{Q}(\sqrt{17})$.

Voor e=4, f=4 krijgen we als basis over $\mathbb{Q}$:

$$\xi_0 = \zeta_0 + \zeta_4 + \zeta_8 + \zeta_{12} = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^4 .$$

$$\xi_1 = \zeta^3 + \zeta^5 + \zeta^{-3} + \zeta^{-5}$$

$$\xi_2 = \zeta^{-8} + \zeta^{-2} + \zeta^8 + \zeta^2$$

$$\xi_3 = \zeta^{-7} + \zeta^{-6} + \zeta^7 + \zeta^6 .$$

Hieruit volgt $\xi_0 + \xi_2 = \eta_0$, $\xi_1 + \xi_3 = \eta_1$, $\xi_0 \xi_2 = \eta_0 + \eta_1 = -1$, $\xi_1 \xi_3 = -1$.

Dus ξ_0 en ξ_2 zijn de wortels van $t^2 - \eta_0 t - 1 = 0$, ξ_1 en ξ_3 van $t^2 - \eta_1 t - 1 = 0$. Daarmee is K_4 bepaald.

Voor $e = 8$, $f = 2$, rekenen we alleen de basiselementen ρ_0 en ρ_4 uit :

$$\rho_0 = \zeta + \zeta^{-1}$$
$$\rho_4 = \zeta^4 + \zeta^{-4} .$$

Dan is $\rho_0 + \rho_4 = \xi_0$, $\rho_0\rho_4 = \xi_1$. Dus zijn ρ_0 en ρ_4 de wortels van $t^2 - \xi_0 t + \xi_1 = 0$.

ζ voldoet aan de vergelijking

$$\zeta + \zeta^{-1} = \rho_0 ,$$

dus

$$\zeta^2 - \rho_0\zeta + 1 = 0.$$

ζ kan dus berekend worden door successive oplossing van een serie vierkantsvergelijkingen. Op de meetkundige betekenis hiervan komen we in § 22 terug.

Opgaven.

1. Bewijs met behulp van (19.3)(i) achtereenvolgens :

(i) $\Phi_2(X) = X + 1$;

(ii) $\Phi_3(X) = X^2 + X + 1$;

(iii) $\Phi_4(X) = X^2 + 1$;

(iv) $\Phi_6(X) = X^2 - X + 1$;

(v) $\Phi_{12}(X) = X^4 - X^2 + 1$.

2. Veronderstel n oneven. Zij ζ een primitieve n-de eenheidswortel, ε een primitieve 2n-de eenheidswortel over $\mathbb{Q}$. Laat zien dat $\mathbb{Q}(\zeta) = \mathbb{Q}(\varepsilon)$.

3. Bepaal de deellichamen van het cirkeldelingslichaam dat de 5-de eenheidswortels van $\mathbb{Q}$ bevat.

20. Cyclische uitbreidingen.

Een Galoisuitbreiding L van K heet cyclisch als de Galoisgroep van L over K cyclisch is.

(20.1) Stelling. K een lichaam, n een natuurlijk getal, $kar(K) = 0$ of $kar(K) = p$, $p \nmid n$. Veronderstel dat K de n-de eenheidswortels over K bevat. Dan geldt :

(i) Voor $a \in K$ is het splijtlichaam van $X^n - a$ over K een cyclische uitbreiding van K. $|L : K|$ is een deler van n. $|L : K| = n \Leftrightarrow X^n - a$ irreducibel in $K[X]$.

(ii) Is L een cyclische uitbreiding van K, $|L : K| = n$, dan is

$L = K(\alpha)$, $\alpha^n = a$, $a \in K$.

Bewijs. (i) Zij α een wortel van $X^n - a$ over K.
Als $\zeta \in K$ een primitieve n-de eenheidswortel is, dan zijn $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha$ n verschillende wortels van $X^n - a$ in $K(\alpha)$, dus $K(\alpha)$ is splijtlichaam van $X^n - a$, dus een Galoisuitbreiding van K.
Zij $\sigma \in G = G_{L/K}$. Dan $\sigma(\alpha) = \chi(\sigma)\alpha$, waarin $\chi(\sigma)$ een n-de eenheidswortel is. Aangezien

$$\chi(\sigma\tau)\alpha = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \chi(\sigma)\chi(\tau)\alpha ,$$

is χ een homomorfisme van G in de cyclische groep van n-de eenheidswortels in K. Uit $\chi(\sigma) = 1$ volgt $\sigma(\alpha) = \alpha$, dus $\sigma = 1$, dus χ is zelf een isomorfisme. Dus is G een cyclische groep waarvan de orde een deler is van n. $|K(\alpha) : K| = n$ dan en slechts dan als $X^n - a$ minimumpolynoom is van α, d.w.z. als $X^n - a$ irreducibel is over K.
(ii) Stel $G = G_{L/K}$, σ een voortbrengende van G. Zij ζ een primitieve n-de eenheidswortel in K. Voor $\xi \in L$ vormen we

$$\eta(\xi) = \xi + \zeta\sigma(\xi) + \zeta^2\sigma^2(\xi) + \ldots + \zeta^{n-1}\sigma^{n-1}(\xi).$$

Aangezien $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ lineair onafhankelijk zijn over L (stelling van Dedekind), is er een $\xi_0 \in L$ zodat $\eta = \eta(\xi_0) \neq 0$.
Nu is

$$\sigma(\eta) = \sigma(\xi_0) + \zeta\sigma^2(\xi_0) + \ldots + \zeta^{n-2}\sigma^{n-1}(\xi_0) + \zeta^{n-1}\xi_0$$
$$= \zeta^{-1}\eta .$$

Algemeen is dus $\sigma^{\nu}(\eta) = \zeta^{-\nu}\eta$.
Noem $\eta^n = a$.

$$\sigma(a) = \sigma(\eta^n) = \sigma(\eta)^n = \zeta^{-n}\eta^n = a ,$$

dus $a \in K$. η is dus een wortel van $X^n - a \in K[X]$.
Voor $\nu = 1, 2, \ldots, n-1$ is $\sigma^{\nu}(\eta) = \zeta^{-\nu}\eta \neq \eta$, dus η is onder geen enkel K-automorfisme $\neq 1$ van L invariant. Derhalve is $L = K(\eta)$.
De structuur van een willekeurige cyclische uitbreiding kan men afleiden met behulp van de twee behandelde gevallen (20.1) en (20.3). Stel L is een cyclische uitbreiding van K van de graad n. Is $kar(K) = 0$, dan zijn we met (20.1) klaar. Is $kar(K) = p$, dan schrijven we $n = p^s n_1$, $p \nmid n_1$. Zij G de Galoisgroep van L over K, σ een voortbrengende van G. Stel $s \geq 1$. Het invariantielichaam M van de ondergroep $\langle \sigma^p \rangle$ is een cyclische uitbreiding van K met $|M : K| = p$, waarvan de structuur dus met (20.3) bepaald kan worden. L is een cyclische uitbreiding van M met

graad $p^{s-1} n_1$. Dit proces herhalen we tot we beland zijn bij een tussenlichaam N zodat L cyclisch is over N met graad n_1; dan zitten we in 't geval van (20.1). Omgekeerd is het natuurlijk niet zo dat een serie uitbreidingen van de in (20.1) en (20.3) behandelde typen cyclisch is; een Galoisuitbreiding van een Galoisuitbreiding hoeft immers niet eens normaal te zijn!
We willen verder een stelling van Hilbert over cyclische uitbreidingen bewijzen; we doen dit in een iets algemener kader.
Zij L een Galoisuitbreiding van K met Galoisgroep G.
Een <u>gekruist homomorfisme van G in L</u> is een afbeelding van G in L^* : $\sigma \to \alpha_\sigma$, met de eigenschap

$$\alpha_{\sigma\tau} = \alpha_\sigma \sigma(\alpha_\tau) .$$

(20.4) <u>Stelling</u>. L Galoisuitbreiding van K met Galoisgroep G. Dan is de afbeelding $\sigma \to \alpha_\sigma$ een gekruist homomorfisme van G in L dan en slechts dan als er een $\lambda \in L$ bestaat zodat $\alpha_\sigma = \lambda^{-1}\sigma(\lambda)$ voor alle $\sigma \in G$.

<u>Bewijs</u>. Is $\alpha_\sigma = \lambda^{-1}\sigma(\lambda)$, $\sigma \in G$, dan is

$$\alpha_{\sigma\tau} = \lambda^{-1}\sigma\tau(\lambda) = \lambda^{-1}\sigma(\lambda)\,\sigma(\lambda^{-1}\tau(\lambda)) = \alpha_\sigma \cdot \sigma(\alpha_\tau) .$$

Stel omgekeerd $\sigma \to \alpha_\sigma$ is een gekruist homomorfisme. Wegens de stelling van Dedekind moet er een $\omega \in L$ bestaan zodat

$$\mu = \sum_{\sigma \in G} \alpha_\sigma \sigma(\omega) \neq 0 .$$

Nu is

$$\sigma(\mu) = \sum_{\tau \in G} \sigma(\alpha_\tau)\,\sigma\tau(\omega)$$

$$= \sum_{\tau \in G} \alpha_\sigma^{-1}\alpha_{\sigma\tau}\,\sigma\tau(\omega)$$

$$= \alpha_\sigma^{-1} \sum_{\rho \in G} \alpha_\rho\,\rho(\omega)$$

$$= \alpha_\sigma^{-1}\mu$$

Dus $\alpha_\sigma = \mu\,\sigma(\mu^{-1})$ voor alle σ.
Met $\lambda = \mu^{-1}$ zijn we er dus.

(20.5) <u>Stelling</u>. (<u>"Stelling 90" van Hilbert</u>). L cyclische uitbreiding van K met Galoisgroep G, σ een voortbrengende van G. Dan is voor $x \in L$, $N_{L/K}(x) = 1$ dan en slechts dan als er een $y \in L$ bestaat zodat $x = y^{-1}\sigma(y)$.

<u>Bewijs</u>. Voor $y \in L$ is $N_{L/K}(y^{-1}\sigma(y)) = N_{L/K}(y)^{-1}N_{L/K}(y) = 1$.

Zij omgekeerd $N(x) = 1$. G bestaat uit de automorfismen $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ als $n = |L:K|$. Stel

$$\alpha_{\sigma^i} = x\,\sigma(x)\sigma^2(x) \dots \sigma^{i-1}(x), \quad 1 \leq i < n,$$
$$\alpha_1 = 1.$$

We beweren dat $\sigma^i \to \alpha_{\sigma^i}$ een gekruist homomorfisme is van G in L. Is n.l. $i+j < n$, dan

$$\alpha_{\sigma^i\sigma^j} = \alpha_{\sigma^{i+j}} = x\,\sigma(x)\dots\sigma^{i-1}(x)\ \sigma^i(x\,\sigma(x)\dots\sigma^{j-1}(x))$$
$$= \alpha_{\sigma^i}\ \sigma^i(\alpha_{\sigma^j}).$$

Stel nu $i+j \geq n$. Wegens $i < n$, $j < n$ is $i+j < 2n$. Dus

$$\alpha_{\sigma^i\sigma^j} = \alpha_{\sigma^{i+j-n}} = x\,\sigma(x)\dots\sigma^{i+j-n}(x)$$

Nu is
$$1 = N_{L/K}(x) = x\sigma(x)\sigma^2(x)\dots\sigma^{n-1}(x), \quad \text{dus}$$

$$\alpha_{\sigma^i\sigma^j} = x\,\sigma(x)\dots\sigma^{i+j-n}(x)\ \sigma^{i+j-n+1}(x\sigma(x)\dots\sigma^{n-1}(x))$$
$$= x\,\sigma(x)\dots\sigma^{i+j}(x)$$
$$= \alpha_{\sigma^i}\ \sigma^i(\alpha_{\sigma^j}).$$

Dus voor $\rho, \tau \in G$ is inderdaad $\alpha_{\rho\tau} = \alpha_\rho\,\rho(\alpha_\tau)$. Er is dus een $y \in L$ zodat $\alpha_\rho = y^{-1}\rho(y)$ voor alle ρ. In het bizonder is

$$x = \alpha_\sigma = y^{-1}\,\sigma(y).$$

Voorbeeld. $\mathbb{C}$ is een Galoisuitbreiding van de graad 2 van $\mathbb{R}$, dus cyclisch van orde 2. $z \to \bar{z}$ is een $\mathbb{R}$-automorfisme $\sigma \neq 1$ van $\mathbb{C}$, dus $G_{\mathbb{C}/\mathbb{R}}$ bestaat uit 1 en σ. Voor $x, y \in \mathbb{R}$ is $N_{\mathbb{C}/\mathbb{R}}(x+iy) = x^2+y^2$. Is $x^2+y^2 = 1$, dan volgt uit de stelling van Hilbert dat er $u, v \in \mathbb{R}$ bestaan zodat $x+iy = \dfrac{u-iv}{u+iv} = \dfrac{(u-iv)^2}{u^2+v^2}$.

Dus $x = \dfrac{u^2-v^2}{u^2+v^2}$, $y = -\dfrac{2uv}{u^2+v^2}$.

Als toepassing van (20.5) bewijzen we tenslotte

(20.6) Stelling. Stel K is een eindig lichaam, L een uitbreiding van K met $|L:K| < \infty$. Dan is er bij iedere $x \in K$ een $y \in L$ zodat $x = N_{L/K}(y)$.

Bewijs. Uit de eindigheid van K volgt dat L een cyclische uitbreiding van K is.

$$N : y \to N_{L/K}(y)$$

is een homomorfisme van L^* in K^*. De kern van N bestaat uit de y met $N_{L/K}(y) = 1$, dus van de vorm $z^{-1}\sigma(z)$, als σ een voortbrengende van $G_{L/K}$ is.

Stel $K = \mathbb{F}_q$, dan kunnen we voor σ het automorfisme

$$\sigma : z \to z^q$$

nemen. De kern van N bestaat dus uit de elementen z^{q-1}, $z \in L$. Is $p = \text{kar}(K)$, dan is $p \nmid q-1$. K bevat alle (q-1)-ste eenheidswortels, n.l. de elementen van K^*, dus volgens (20.1) is het aantal oplossingen in L van de vergelijking $z^{q-1} - a = 0$ nul of precies q-1. Het aantal elementen van de kern van N bedraagt dus $|L^*|(q-1)^{-1}$. Het beeld van L^* bestaat dus uit q-1 elementen, d.w.z. uit de hele K^*.

Opgave.

1. Bewijs met een redenering analoog aan die na het bewijs van (20.3), bij de beschouwing van willekeurige cyclische uitbreidingen, de volgende bewering:
Is L een cyclische uitbreiding van K, dan zijn er lichamen K_i zodat $K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_{s-1} \subset K_s = L$ zodat K_i een cyclische uitbreiding is van K_{i-1} met $|K_i : K_{i-1}|$ priem, voor i=1,...,s.

21. Oplosbare vergelijkingen.

Een separabele uitbreiding L van K met $|L : K| < \infty$ heet oplosbaar als er keten tussenlichamen bestaat : $K=K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n = L$ zodat K_i een cyclische (Galois-)uitbreiding is van K_{i-1} voor $1 \leq i \leq n$. De keten tussenlichamen $K=K_0 \subset K_1 \subset \ldots \subset K_n = L$ heet een cyclische toren tussen K en L, de graden $|K_i : K_{i-1}|$, $1 \leq i \leq n$, heten de graden van de cyclische toren.
Merk op dat er bij een oplosbare uitbreiding verschillende cyclische torens kunnen zijn met verschillende graden.

(21.1) Hulpstelling. Zij L een Galoisuitbreiding van K, $|L : K| < \infty$, L' een uitbreiding van L die een deellichaam $K' \supset K$ bevat zodat $L' = K'L$. Dan is L' een Galoisuitbreiding van K', $|L':K'| < \infty$ en $G_{L'/K'}$ is isomorf met een ondergroep van $G_{L/K}$.

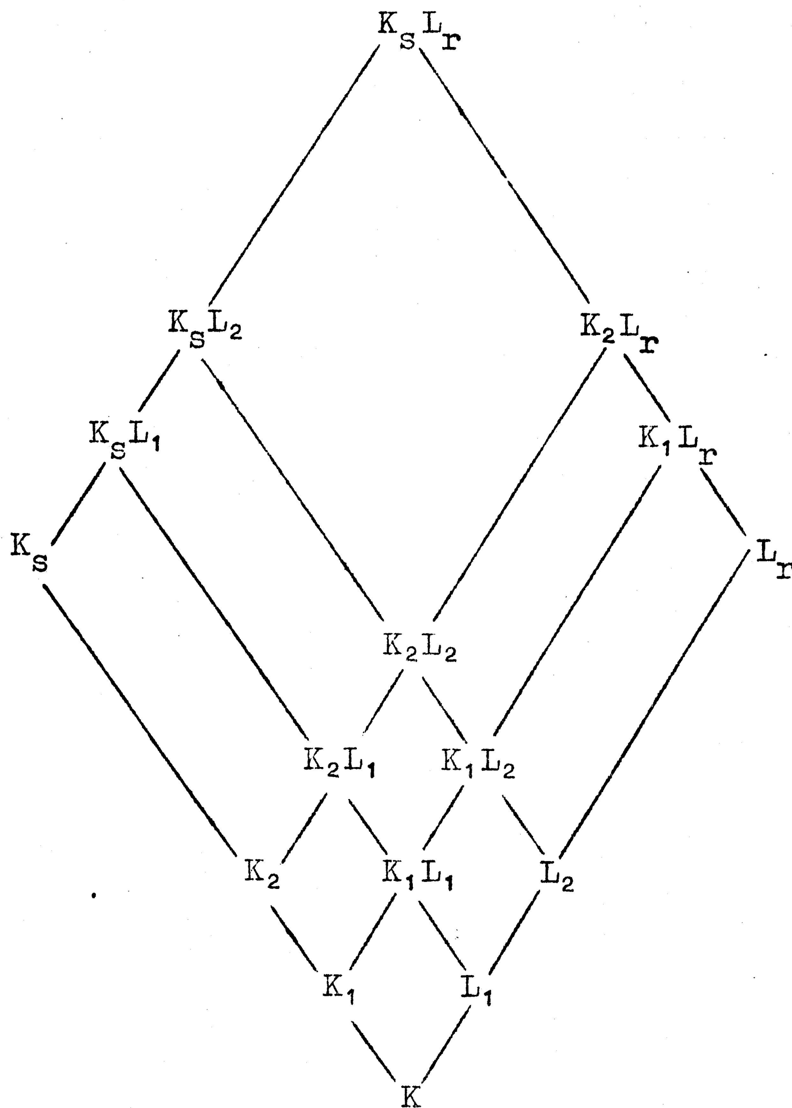
Bewijs. L is splijtlichaam over K van een separabele veelterm

$f\in K[X]$. Laat $x_1,\dots,x_n$ de wortels van f in L zijn; dus $L=K(x_1,\dots,x_n)$. Omdat $L'=K'L$, is $L'=K'(x_1,\dots,x_n)$. L' is dus splijtlichaam over K' van de separabele veelterm $f\in K'[X]$, dus L' is een Galoisuitbreiding van K' en $|L':K'|<\infty$.

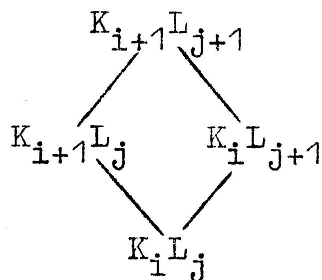
Stel $\sigma'\in G_{L'/K'}$. σ' permuteert $x_1,\dots,x_n$. Omdat $K\subset K'$ en $\sigma'|K'=1$, is ook $\sigma'|K=1$. Dus σ' induceert een K-automorfisme σ van $L:\sigma=\sigma'|L$. $\sigma'\to\sigma$ is een homomorfisme van $G_{L'/K'}$ in $G_{L/K}$. Als $\sigma=1$, dan $\sigma(x_i)=x_i$, $i=1,\dots,n$, dus $\sigma'(x_i)=x_i$, $i=1,\dots,n$, dus $\sigma'=1$. Dus $\sigma'\to\sigma$ is zelfs een isomorfisme.

(21.2) Stelling. Gegeven een cyclische toren $K=K_0\subset K_1\subset\dots\subset K_s$, met K_s separabel over K. Dan bestaat er een cyclische toren $K=K_0\subset K_1\subset\dots\subset K_s\subset K_{s+1}\subset\dots\subset K_t$, zodat K_t de normale afsluiting van K_s over K is en zodat alle graden van de tweede toren voorkomen onder de delers van de graden van de eerste toren.
De normale afsluiting van een oplosbare uitbreiding van K is dus een oplosbare Galoisuitbreiding.

Bewijs. K_s is een separabele uitbreiding van K, dus $K_s=K(\alpha)$. Zij f het minimumpolynoom van α over K. Neem een splijtlichaam L van f over K_s ; L is tevens splijtlichaam van f over K. f is separabel, dus L is een Galoisuitbreiding van K. Zij G de Galoisgroep van L over K. $\prod_{\sigma\in G}\sigma(K_s)$ is een deellichaam van L dat alle wortels van f bevat, dus $\prod_{\sigma\in G}\sigma(K_s)=L$. Voor iedere $\sigma\in G$ is $K=K_0\subset\sigma(K_1)\subset\sigma(K_2)\subset\dots\subset\sigma(K_s)$ een cyclische toren met dezelfde graden als de toren $K_0\subset K_1\subset\dots\subset K_s$. We moeten dus bewijzen dat het compositum van cyclische torens weer een cyclische toren is, waarvan de graden delers zijn van die van de gegeven torens. Het is uiteraard voldoende dit voor twee torens te bewijzen. Stel dus we hebben twee cyclische torens $K=K_0\subset K_1\subset\dots\subset K_s$ en $K=L_0\subset L_1\subset\dots\subset L_r$, zodat K_s en L_r bevat zijn in een lichaam M. We hebben dan in M het volgende patroon van deellichamen :



Stel we weten dat in een "cel" van het patroon



$K_{i+1}L_j$ en K_iL_{j+1} cyclische uitbreidingen zijn van K_iL_j . Uit (21.1) volgt dat $K_{i+1}\ L_{j+1}$ een Galoisuitbreiding is van

K_iL_{j+1} waarvan de Galoisgroep isomorf is met een ondergroep van de Galoisgroep van $K_{i+1}L_j$ over K_iL_j. Dus $K_{i+1}L_{j+1}$ is een cyclische uitbreiding van K_iL_{j+1} en $|K_{i+1}L_{j+1}:K_iL_{j+1}|$ is een deler van $|K_{i+1}L_j : K_iL_j|$. Evenzo is $K_{i+1}L_{j+1}$ cyclisch over $K_{i+1}L_j$ en $|K_{i+1}L_{j+1} : K_{i+1}L_j|$ deelt $|K_iL_{j+1} : K_iL_j|$. Met een simpel inductieprocédé toont men nu verder aan dat alle uitbreidingen $K_iL_j \subset K_iL_{j+1}$ en $K_iL_j \subset K_{i+1}L_j$ in het grote patroon cyclisch zijn en dat hun graden delers zijn van $|L_{j+1} : L_j|$ of $|K_{i+1} : K_i|$ respectievelijk. Daarmee is het bewijs voltooid.

(21.3) Stelling. Zij L een Galoisuitbreiding van K, $|L : K| < \infty$. L is oplosbaar over K dan en slechts dan als $G_{L/K}$ oplosbaar is.

Bewijs. Stel L oplosbaar. Dan is er een toren $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$ zodat K_i cyclisch is over K_{i-1} voor alle i. Noem $G_i = G_{L/K_i}$. Omdat K_i normaal is over K_{i-1}, is G_i normaaldeler van G_{i-1}. K_i is cyclisch over K_{i-1}, dus G_{i-1}/G_i is cyclisch. Daaruit volgt dat $G_{L/K} = G_0$ oplosbaar is.

Is omgekeerd $G_{L/K}$ oplosbaar, dan is er een keten van ondergroepen $G_{L/K} = G_0 \supset G_1 \supset \ldots \supset G_n = (1)$, zodat G_i normaaldeler is van G_{i-1} en G_{i-1}/G_i cyclisch is voor alle $i=1,\ldots,n$. Neem $K_i = \mathrm{Inv}(G_i)$ in L, dan is K_i een cyclische uitbreiding van K_{i-1}, dus L is oplosbaar.

Zij nu f een separabele veelterm in K[X]. f heet oplosbaar over K (door worteltrekken), als er een keten lichamen $K = K_0 \subset K_1 \subset \ldots \subset K_t$ bestaat met $K_i = K_{i-1}(\xi_i), \xi_i^{n_i} = \alpha_i \in K_{i-1}$, voor $1 \leq i \leq t$, zodat f splijt in K_t. Grofweg gezegd betekent dit, dat de wortels van f berekend kunnen worden door rationale operaties en 't trekken van n_i-de machts wortels.

Bij de nu volgende behandeling van oplosbare veeltermen zullen

we veronderstellen dat kar(K) = 0, dit om moeilijkheden met separabiliteit en het bestaan van primitieve eenheidswortels uit de weg te gaan.

(21.4) Stelling. Stel kar(K) = 0, $f \in K[X]$. Zij L een splijtlichaam van f over K. Dan is f oplosbaar dan en slechts dan als $G_{L/K}$ oplosbaar is.

Bewijs. Stel f is oplosbaar. Dan hebben we een keten $K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_t$, met $K_i = K_{i-1}(\xi_i), \xi_i^{n_i} = \alpha_i \in K_{i-1}$, zodat f splijt in K_t.
Neem $N = n_1 n_2 \ldots n_t$. Zij ζ een primitieve N-de eenheidswortel over K, $L_0 = K(\zeta)$. L_0 is een Galoisuitbreiding van K, $G_{L_0/K}$ is commutatief, dus zeker oplosbaar. L_0 is dus een oplosbare uitbreiding van K.
Neem $L_1 = L_0(\xi_1)$, $L_2 = L_1(\xi_2), \ldots, L_t = L_{t-1}(\xi_t)$.
$L_i = L_{i-1}(\xi_i)$, ξ_i is de wortel van $X^{n_i} - \alpha_i \in L_{i-1}[X]$, L_{i-1} bevat de n_i-de eenheidswortels (die zitten n.l. al in L_0), dus L_i is een cyclische uitbreiding van L_{i-1}. L_t is dus oplosbaar over K. De normale afsluiting M van L_t over K is een Galoisuitbreiding van K die volgens (21.2) oplosbaar is. f splijt in K_t, dus zeker in M. We mogen dus aannemen dat het splijtlichaam L van f in M bevat is. $G_{L/K} \cong G_{M/K}/G_{M/L}$. $G_{M/K}$ is oplosbaar, dus z'n factorgroep $G_{L/K}$ is ook oplosbaar.
Veronderstel omgekeerd dat $G_{L/K}$ oplosbaar is. Stel $|L:K| = l$. Neem een primitieve l-de eenheidswortel ε over L. Zij L splijtlichaam over K van $f \in K[X]$. $L(\varepsilon)$ is dan splijtlichaam van $f(X)(X^l - 1)$ over K, dus een Galoisuitbreiding van K, dus ook een Galoisuitbreiding van $K(\varepsilon)$. $G_{L(\varepsilon)/K(\varepsilon)}$ is isomorf met een ondergroep van $G_{L/K}$, dus oplosbaar. We hebben dus een cyclische toren $K(\varepsilon) = K_0 \subset K_1 \subset \ldots \subset K_n = L(\varepsilon)$. K_0 bevat de l-de eenheidswortels, dus K_{i-1} bevat de n_i-de eenheidswortels over K, als $n_i = |K_i : K_{i-1}|$, want $n_i \mid l$. Dus $K_i = K_{i-1}(\xi_i)$, $\xi_i^{n_i} = \alpha_i \in K_{i-1}$.
We hebben dus een keten $K \subset K(\varepsilon) = K_0 \subset K_1 \subset \ldots \subset K_n = L(\varepsilon)$, $K_i = K_{i-1}(\xi_i)$, $\xi_i^{n_i} = \alpha_i \in K_{i-1}$, $K_0 = K(\varepsilon)$, $\varepsilon^l = 1$. f splijt in L, dus in $L(\varepsilon)$. Dus f is oplosbaar over K.

Het onderzoek naar de oplosbaarheid van veeltermen leidt ons tot het probleem van de oplosbaarheid van Galoisgroepen. Aangezien deze op te vatten zijn als ondergroepen van de volle permutatiegroep S_n van de wortels van een veelterm, houden we ons eerst bezig met de oplosbaarheid van de groepen S_n. S_n heeft als normaaldeler A_n, de groep van de even permutaties.
S_n/A_n heeft orde 2, is dus cyclisch. Dus S_n is oplosbaar dan en slechts dan als A_n het is.

(21.5) Stelling. Voor $n=2,3,4$ zijn S_n en A_n oplosbaar. Voor $n>4$ is A_n enkelvoudig (d.w.z. bevat geen normaaldelers) en niet commutatief, dus S_n is niet oplosbaar.

Bewijs. $n=2$: $|S_2|=2$, dus S_2 is 2-cyclisch. $A_2=(1)$.
$n=3$: $|S_3|=6$, $|S_3 : A_3|=2$, dus $|A_3|$ is een 3-cyclische groep. S_3 is dus oplosbaar.
$n=4$: $|S_4|=24$, $|A_4|=12$. Zij V_4 de ondergroep van A_4 voortgebracht door de permutaties 1, (12)(34) , (13)(24) , (14)(23). Ga na dat V_4 normaaldeler is van A_4. $|A_4 : V_4|=3$, dus A_4/V_4 is een 3-cyclische groep.
V_4 bevat de normaaldeler C_2 bestaande uit 1 en (12)(34) .
$|V_4 : C_2|=2$, $|C_2|=2$, dus V_4/C_2 en C_2 zijn 2-cyclisch. $n>4$.
A_n niet commutatief : (12)(34) en (12)(35) commuteren niet, zoals men makkelijk narekent.
We laten het bewijs van de enkelvoudigheid van A_n in verschillende stappen verlopen.
(i) A_n wordt voortgebracht door 3-cycli.
Ieder element van A_n is n.l. product van een even aantal 2-cycli, dus is het voldoende te bewijzen dat een product van twee 2-cycli te schrijven is als product van 3-cycli. Het algemene geval (ij)(kl) behoort tot één van de volgende typen :
(12)(13) = (132)
(12)(34) = (12)(13)(13)(34) = (132)(341)

(ii) Zijn γ_1 en γ_2 3-cycli, dan is er een $\beta \in A_n$ zodat $\beta\gamma_1\beta^{-1}=\gamma_2$. Het is voldoende dit te bewijzen voor $\gamma_1=(123)$ en $\gamma_2=(ijk)$.
Neem een permutatie

$$\beta' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & n & \cdots \end{pmatrix}$$

Is β' even, dan $\beta = \beta'$; is β' oneven, dan $\beta = (1n)\beta'$ (hier gebruiken we dat $n > 4$).
β is dus een even permutatie, die $1 \to i$, $2 \to j$, $3 \to k$, dus $\beta(123)\beta^{-1} = (ijk)$.
(iii) Zij H een normaaldeler in A_n. Uit (ii) volgt onmiddellijk : bevat H een 3-cyclus, dan bevat H alle 3-cycli, dus $H = A_n$ wegens (i).
(iv) Stel H is normaaldeler van $A_n, H \neq 1$. We zullen bewijzen dat H een 3-cyclus bevat. Volgens (iii) is dan $H = A_n$.
Neem $\alpha \neq 1$ in H zodanig dat α zoveel mogelijk getallen uit de verzameling $(1,2,\ldots,n)$ vastlaat.
Laat α n-3 getallen vast, dan is α een 3-cyclus en dan zijn we klaar.

Laat α precies n-4 getallen vast, zeg de getallen $5,6,\ldots,n$, dan moet α van de gedaante $\alpha = (12)(34)$ zijn. Neem $\sigma = (345)$, dan $\alpha_1 = \sigma\alpha\sigma^{-1} = (12)(45)$. $\alpha\alpha_1 = (345)$, dus laat meer getallen vast dan α : tegenspraak.
Stel nu α laat hoogstens n-5 getallen vast. We schrijven α als product van cycli, die geen elementen gemeen hebben; daar deze commuteren, mogen we de langste cyclus voorop schrijven. We hebben dan essentieel drie gevallen :

$$\alpha = (1234\ldots)\ldots$$

of $$\alpha = (123)\ (45\ldots)\ldots\ \ldots$$

of $$\alpha = (12)(34)\ (56)\ldots$$

Neem $\sigma = (234)$, $\alpha_1 = \sigma\alpha\sigma^{-1}$. Dan wordt achtereenvolgens

$$\alpha_1 = (1342\ldots)\ldots$$

of $$\alpha_1 = (134)(25)\ldots)\ldots$$

of $$\alpha_1 = (13)(42)(56)\ldots,$$

waarbij de niet opgeschreven getallen in α_1 dezelfde zijn als in α. In alle gevallen is $\alpha_1 \neq \alpha$, dus $\alpha^{-1}\alpha_1 \neq 1$. In het eerste en derde geval laat $\alpha^{-1}\alpha_1$ alle $k > 4$ vast, dus meer dan α vastlaat : tegenspraak. In het tweede geval laat $\alpha^{-1}\alpha_1$ alle $k > 5$ vast, dus n-5 elementen, terwijl α in dat geval $\leq n-6$ getallen vastlaat, wat minder is : tegenspraak.
Aangezien hiermee alle mogelijkheden uitgeput zijn, concluderen we dat α een 3-cyclus is.

Uit de oplosbaarheid van S_n voor $n \leq 4$ volgt dat iedere f van graad ≤ 4 oplosbaar is als kar(K) = 0. We onderzoeken deze gevallen afzonderlijk.

I. $gr(f) = 2$. $f(X) = aX^2 + bX + c$.

Hier hebben we de welbekende formule voor de wortels :

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} ,$$

die zegt dat f splijt in $K(\sqrt{b^2-4ac})$, dus oplosbaar is.
Deze formule geldt voor alle lichamen K met $kar(K) \neq 2$.

II. $gr(f) = 3$. $f(X) = X^3 + aX^2 + bX + c$.

Door de transformatie $X \to X - \frac{1}{3}a$ krijgen we f in de gedaante

$$f(X) = X^3 + pX + q.$$

Stel een wortel is $x = u+v$, dan is

$$u^3+v^3+3uv(u+v) + p(u+v) + q = 0.$$

Kies u en v zodanig dat $3uv = -p$, dan

$$u^3+v^3 = -q, \quad u^3v^3 = \frac{-p^3}{27} .$$

u^3 en v^3 zijn dus oplossingen van de vierkantsvergelijking

$$t^2 + qt - \frac{p^3}{27} = 0.$$

$$u^3 = -\frac{q}{2} + \frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}} , \quad v^3 = -\frac{q}{2} - \frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}} .$$

Is ζ een primitieve 3-de eenheidswortel over K, dan vinden we dus als wortels

$$x = \zeta^k \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}}} + \zeta^{-k}\sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{q^2+\frac{4p^3}{27}}}$$

met k=1,2,3. Deze formule is geldig over elk lichaam K met kar (K) $\neq 2,3$. In het lichaam van de complexe getallen kunnen we $\zeta = e^{\frac{2\pi i}{3}}$ nemen. Dan krijgen we de klassieke <u>formule van Cardano</u> :

$$x = e^{\frac{2\pi i}{3}k}\sqrt[3]{-\frac{q}{2} + \sqrt{q^2+\frac{4p^3}{27}}} + e^{-\frac{2\pi i}{3}k}\sqrt[3]{-\frac{q}{2} - \sqrt{q^2+\frac{4p^3}{27}}} ,$$

$k = 0,1,2$. Men moet de twee derdemachtswortels die u en v voorstellen zo kiezen, dat $uv = -\frac{1}{3}p$.

III. $gr(f) = 4$. Men kan in dit geval, net als in II, f reduceren tot de gedaante

$$f(X) = X^4 + aX^2 + bX + c.$$

Door eenzelfde soort kunstgrepen als bij II, kan men de wortels $x_1, \dots, x_4$ als volgt bepalen :
Neem voor u^2, v^2, w^2 de drie oplossingen van

$$z^3 + 2az^2 + (a^2 - 4c)z - b^2 = 0 \ ,$$

die (na eliminatie van de term met z^2) met de formule van Cardano berekend kunnen worden. Door worteltrekken vinden we dan u,v en w, die van zodanige tekens voorzien moeten worden dat $uvw = -b$. Dan is

$$2x_1 = u+v+w$$
$$2x_2 = u-v-w$$
$$2x_3 = -u+v-w$$
$$2x = -u-v+w.$$

Deze formules gelden weer over elke K met $kar(K) \neq 2,3$. Voor de afleiding zij verwezen naar het in de literatuurlijst genoemde werk van H.Weber, deel I, blz. 135-6.

Zij K een willekeurig commutatief lichaam. Onder de algemene n-de graads veelterm over K verstaan we

$$f(X) = X^n - u_1X^{n-1} + u_2X^{n-2} - \dots + (-1)^n u_n$$

waarin $u_1, \dots, u_n$ algebraïsch onafhankelijk zijn over K.

(21.6) Stelling. Zij $f(X) = X^n - u_1X^{n-1} + \dots + (-1)^n u_n$ de algemene veelterm over K, $L = K(u_1, \dots, u_n)$, M het splijtlichaam van f over L. Dan geldt :

(i) f is irreducibel in $L[X]$.
(ii) f is separabel.
(iii) $G_{M/L} \cong S_n$.

Bewijs. (ii) is duidelijk omdat bijvoorbeeld $u_{n-1} \neq 0$, dus f is niet te schrijven als een polynoom in X^p .
(i) volgt uit (iii). Was n.l. f reducibel, dan f=gh met $gr(g)=k$, $gr(h)=l$, $k+l=n$, $1 < k,l < n$. Dan $|M : L| \leq k! + l! < n! = |G_{M/L}|$, tegenspraak.
Bewijzen we nu dus (iii). Stel $v_1, \dots v_n$ zijn de wortels van f in M. Uit

$$(X-v_1)(X-v_2)\dots(X-v_n) = X^n - u_1X^{n-1} + \dots + (-1)^n u_n$$

volgt

$$u_i = \sum_{1 \le j_1 < j_2 < \ldots < j_i \le n} v_{j_1} v_{j_2} \ldots v_{j_i} \quad .$$

Dus $K(v_1, \ldots, v_n) = K(u_1, \ldots, u_n, v_1, \ldots, v_n) = M$.

Vergelijking van de transcendentiegraden levert wegens (7.3)

$$\begin{aligned} \text{trgr}(M : K) &= \text{trgr}(M : L) + \text{tr}(L : K) \\ &= \quad 0 \quad + \quad n \\ &= n. \end{aligned}$$

Daaruit volgt dat $v_1, \ldots, v_n$ algebraïsch onafhankelijk zijn over K. Iedere permutatie van $v_1, \ldots, v_n$ is dus voort te zetten tot een K-automorfisme σ van M. Omdat de u_i symmetrische veeltermen zijn in $v_1, \ldots, v_n$, is iedere u_i invariant onder σ. σ is dus zelfs een L-automorfisme van M. Daaruit volgt dat $G_{M/L}$, opgevat als permutatiegroep van de wortels $v_1, \ldots, v_n$, alle permutaties bevat, dus $G_{M/L} \cong S_n$.

Een onmiddellijk gevolg van deze stelling en (21.5) is

(21.7) Stelling (Abel-Ruffini). Is $\text{kar}(K) = 0$, dan is de algemene vergelijking van graad > 4 over K niet oplosbaar.

Voor vergelijkingen van de graad > 4 kunnen dus geen algemene formules bestaan die de wortels in de coëfficiënten uitdrukken, analoog aan bijv. de formule van Cardano voor derdegraads vergelijking.

We blijven nog even bij de algemene veelterm van de graad n over K :

$$f(X) = X^n - u_1 X^{n-1} + u_2 X^{n-2} - \ldots + (-1)^n u_n \quad .$$

$L = K(u_1, \ldots, u_n)$, M = splijtlichaam van f over L, $v_1, \ldots, v_n$ wortels van f in M. De grootheid

$$\Delta = \prod_{i<j} (v_i - v_j)$$

is invariant onder even permutaties van de wortels en gaat over in $-\Delta$ onder oneven permutaties. Dus $L(\Delta)$ is een uitbreiding van L zodat $G_{M/L(\Delta)} \cong A_n$. Daaruit volgt dat $|L(\Delta) : L| = 2$.

$$D = \Delta^2 = \prod_{i<j} (v_i - v_j)^2$$

is invariant onder alle permutaties van de wortels, dus $D \in K$. Dus $K(\Delta) = K(\sqrt{D})$. D heet de discriminant van f.

D is een symmetrische functie van $v_1, \dots, v_n$. We willen aantonen dat D een veelterm is in $u_1, \dots, u_n$. Daartoe moeten we eerst iets over symmetrische veeltermen bewijzen.

$f \in K[X_1, \dots, X_n]$ heet een symmetrische veelterm, als $f(X_{\pi(1)}, \dots, X_{\pi(n)}) = f(X_1, \dots, X_n)$ voor elke permutatie $\pi \in S_n$.
Voorbeelden hiervan zijn de polynomen

$$f_i(X_1, \dots, X_n) = \sum_{1 \leq j_1 < \dots < j_i \leq n} X_{j_1} \dots X_{j_i} \;, \; 1 \leq i \leq n \;.$$

Deze heten de elementaire symmetrische veeltermen.

(21.8) Stelling. Zij f een symmetrische veelterm $\in K[X_1, \dots, X_n]$. Dan is er een $h \in K[X_1, \dots, X_n]$ zodat

$$f(X_1, \dots, X_n) = h(f_1(X_1, \dots, X_n), f_2(X_1, \dots, X_n), \dots, f_n(X_1, \dots, X_n)).$$

Bewijs. Als totale graad van een monoom (eenterm)

$$a\, X_1^{k_1} X_2^{k_2} \dots X_n^{k_n} \;, \quad a \neq 0 \;,$$

definiëren we $k_1 + k_2 + \dots + k_n$.

Een veelterm heet homogeen, als al z'n monomen dezelfde totale graad hebben. Een veelterm f is som van homogene veeltermen. Een permutatie van $X_1, \dots, X_n$ voert ieder monoom in f over in een monoom van dezelfde graad. Is f symmetrisch, dan zijn de homogene delen van f dus ook symmetrisch.

We mogen dus verder aannemen dat f homogeen en symmetrisch is. De monomen in f ordenen we lexicografisch :

$a\, X_1^{k_1} \dots X_n^{k_n} > b\, X_1^{l_1} \dots X_n^{l_n}$ als er een t is, $1 \leq t \leq n$, zodat $k_1 = l_1$, $k_2 = l_2, \dots, k_{t-1} = l_{t-1}$, $k_t > l_t$.

Laat nu $a\, X_1^{k_1} \dots X_n^{k_n}$ het grootste monoom zijn in f onder de lexicografische ordening. f bevat alle monomen die ontstaan door permutaties van $X_1, \dots, X_n$, dus moet $k_1 \geq k_2 \geq \dots \geq k_n$.
Neem nu het hoogste monoom in de symmetrische veelterm

$$f_1^{d_1} f_2^{d_2} \dots f_n^{d_n} \;;$$

deze is

$$X_1^{d_1+d_2+\dots+d_n} X_2^{d_2+\dots+d_n} \dots X_n^{d_n} .$$

Dus

$$a f_1^{k_1-k_2} f_2^{k_2-k_3} \dots f_n^{k_n}$$

heeft hetzelfde grootste monoom als f. Daaruit volgt dat het hoogste monoom in

$$f_1 = f - af_1^{k_1-k_2} \dots f_n^{k_n}$$

lager is dan dat in f. Herhaal het bovenstaande procédé met f_1. Na eindig veel stappen breekt het af, aangezien er slechts eindig veel symmetrische veeltermen zijn met een hoogste monoom dat kleiner is dan $X_1^{k_1} \dots X_n^{k_n}$ (op een factor uit K na natuurlijk).
Dus is f een polynoom in $f_1,\dots,f_n$.

We keren nu terug tot de discriminant D. D is symmetrisch in $v_1,\dots,v_n$, dus is een veelterm in de $f_i(v_1,\dots,v_n) = u_i$.
In het algemeen is D moeilijk te berekenen. In enige eenvoudige gevallen lukt het wel.

I. $f(X) = X^2 - u_1X + u_2$.

$$D = (v_1 - v_2)^2 = (v_1 + v_2)^2 - 4v_1 v_2$$
$$= u_1^2 - 4u_2 .$$

$A_2 = (1)$, dus $L(\sqrt{D}) = M$. Dus f splijt in $L(\sqrt{D})$. Inderdaad zijn de wortels

$$\tfrac{1}{2} u_1 \pm \tfrac{1}{2} \sqrt{D} .$$

II. $f(X) = X^3 + pX + q$.
Hier is

$$v_1 + v_2 + v_3 = 0$$
$$v_1v_2 + v_1v_3 + v_2v_3 = p$$
$$v_1v_2v_3 = -q$$

Hieruit is af te leiden

$$D = (v_1 - v_2)^2 (v_2 - v_3)^2 (v_1 - v_3)^2$$
$$= -4p^3 - 27q^2 .$$

Vult men voor p en q elementen uit K in, dan is de Galoisgroep G van het splijtlichaam over K, S_3 of A_3 , aangenomen althans dat f dan irreducubel is.

$G = S_3 \Leftrightarrow A_3 \neq G \Leftrightarrow \mathrm{Inv}(A_3) \neq \mathrm{Inv}(G) \Leftrightarrow K(\sqrt{D}) \neq K \Leftrightarrow D$ is geen kwadraat in K.
Hiermee hebben we dus een criterium bij de hand om na te gaan of het splijtlichaam van f van de graad 3 of 6 is!

De formule voor de wortels van de algemene veelterm

$$f(X) = X^3 + pX + q$$

kan men als volgt vinden. Adjungeer eerst $\sqrt{D}$ aan K.
$D = -4p^3 - 27q^2$. Zij ε een primitieve derde eenheidswortel, bijv.

$$\varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}\ ;\ \text{dan is}\ \varepsilon^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-3}\ .$$

Stel nu

$$s_i = v_1 + \varepsilon^i v_2 + \varepsilon^{2i} v_3,\ i=0,1,2.$$

Dan is $s_0 = 0$. Reken na, dat

$$s_1^3 = -\frac{27}{2} q + \frac{3}{2}\sqrt{-3D}\ ,$$

$$s_2^3 = -\frac{27}{2} q - \frac{3}{2}\sqrt{-3D}\ .$$

Voor s_1 kan men nu elk van de drie mogelijke derdemachtswortels uit s_1^3 kiezen - die een derde eenheidswortel verschillen. s_2 is dan bepaald als de derdemachtswortel uit s_2^3 die voldoet aan

$$s_1 s_2 = -3p\ .$$

Hieruit vindt men de wortels v_1, v_2 en v_3. Het uiteindelijke resultaat levert weer de formule van Cardano. Ga dit zelf na.

Voor de algemene derdegraads veelterm

$$f(X) = X^3 - u_1 X^2 + u_2 X - u_3$$

vindt men als discriminant

$$D = -4u_1^3 u_3 + u_1^2 u_2^2 + 18 u_1 u_2 u_3 - 4u_2^3 - 27u_3^2\ .$$

Tracht dit zelf af te leiden, hetzij rechtstreeks zoals in het bewijs van (21.8), hetzij door eerst de veelterm te reduceren tot één van het type $X^3 + pX + q$. De afleiding is ook te vinden bij Jacobson (zie literatuurlijst) deel III, p.93.

22. Constructies met passer en lineaal.

Zij K een commutatief lichaam met karakteristiek $\neq 2$, V het affiene vlak over K.
Een coördinatenstelsel in V wordt vastgelegd door de keuze van de punten (0,0) , (1,0) en (0,1).
Door constructies met de lineaal alleen - waarbij we het trekken van evenwijdige lijnen toelaten - kunnen we elk punt (x,y) con-

strueren met x en y in het priemlichaam P van K. Dus $P=\mathbb{Q}$ als $kar(K)=0$, $P=\mathbb{F}_p$ als $kar(K)=p$.
Constructies met de lineaal komen neer op het oplossen van stelsels lineaire vergelijkingen. Gebruiken we ook een passer, dan komen er snijpunten van cirkels en rechten bij. De coördinaten daarvan zijn oplossingen van vierkantsvergelijkingen. Omgekeerd komt het oplossen van een willekeurige vierkantsvergelijking neer op het snijden van een cirkel met een rechte. Daarbij treden dus in het algemeen kwadratische lichaamsuitbreidingen op.
Zij gegeven in het vlak V de punten (0,0) , (1,0) en (0,1) en een aantal punten en lijnen waarvan de coördinaten zijn $a_1, a_2, \ldots, a_n$. Met de lineaal alleen zijn alle punten en lijnen te construeren met coördinaten in $L=P(a_1,\ldots,a_n)$. Een punt of lijn is met de passer en de lineaal te construeren dan en slechts dan als z'n coördinaten in een uitbreiding M van L liggen die door een toren van kwadratische uitbreidingen uit L verkregen kan worden :

$$L=L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_t = M \ ,$$

$|L_i : L_{i-1}| = 2.$

Volgens stelling (21.2) is de normale afsluiting N van M over L ook uit L te verkrijgen door een toren van kwadratische uitbreidingen. Dan is dus $|N:L| = 2^s$. N is een Galoisuitbreiding van L aangezien $kar(L)\neq 2$.
Zij omgekeerd gegeven dat α element is van een Galoisuitbreiding N van L met $|N:L| = 2^s$.
$|G_{N/L}| = 2^s$, dus $G_{N/L}$ is oplosbaar (zie dictaat Groepentheorie):
$G_{N/L} = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_s = (1)$,
G_i normaaldeler in G_{i-1} , G_{i-1}/G_i cyclisch van de orde 2.
Neem $L_i = Inv(G_i)$. Dan is

$$L=L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_s = N \ ,$$

L_i kwadratische uitbreiding van L_{i-1} . Dus ieder element van N is door constructies met passer en lineaal te verkrijgen uit L, d.w.z. uit de gegevens van het probleem. Daarmee hebben we de volgende stelling bewezen.

(22.1) Stelling. Zij P het priemlichaam van karakteristiek $\neq 2$. Stel in het affiene vlak zijn grootheden $a_1,\ldots,a_n$ gegeven (als co-

ördinaten van punten of lijnen) en de punten (0,0) , (1,0) , (0,1). $L = P(a_1, \ldots, a_n)$.
Voor de construeerbaarheid van een grootheid α met passer en lineaal is dan
(i) noodzakelijk en voldoende dat $L(\alpha)$ uit L te verkrijgen is door een serie kwadratische uitbreidingen;
(ii) noodzakelijk en voldoende dat α in een Galoisuitbreiding N van L ligt met $|N : L| = 2^s$, $s \geq 0$;
(iii) noodzakelijk dat $|L(\alpha) : L| = 2^t$, $t \geq 0$.

N.B. Is $P = \mathbb{Q}$, en is $\alpha \in \mathbb{R}$, dan kan het gebeuren dat één van de tussenstappen bij de constructie van α niet reëel is. Bovenstaande stelling garandeert dus niets over de construeerheid in het reële vlak.

We passen het bovenstaande toe op een aantal klassieke constructieproblemen in het geval $\mathrm{kar}(P) = 0$. Dan is dus $P = \mathbb{Q}$, het lichaam van de rationale getallen. Met "construeren" etc. bedoelen we verder : "construeren met passer en lineaal" etc.

I. Verdubbeling van de kubus.
Gegeven een kubus. Vraag : kan men een kubus construeren met dubbele inhoud.
Neem de ribbe van de kubus als lengte-eenheid. Het probleem komt dan neer op het construeren van $\sqrt[3]{2}$, d.w.z. van een wortel van $X^3 - 2$.
$X^3 - 2$ heeft geen wortels in $\mathbb{Q}$ (waarom niet?) , dus is irreducibel over $\mathbb{Q}$, want z'n graad is 3. Is α een wortel van $X^3 - 2$, dan is $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$, wat geen macht van 2 is. Deze constructie is dus niet mogelijk.

II. Trisectie van de hoek.
Gegeven een willekeurige hoek α. Construeer $\frac{1}{3}\alpha = \theta$. Dit komt neer op de bepaling van $\cos\theta$, als $\cos\alpha$ gegeven is. Omdat $\alpha = 3\theta$, is

$$\cos\alpha = 4\cos^3\theta - 3\cos\theta.$$

$\cos\theta$ is dus wortel van

$$f(X) = 4X^3 - 3X - \cos\alpha.$$

Als deze veelterm reducibel is over $\mathbb{Q}$, dus een wortel heeft in

$\mathbb{Q}$, dan moet cos α in elk geval rationaal zijn, dus voor de "meeste" waarden van α is f irreducibel. Ook voor rationale waarden van cos α kan nog wel irreducibiliteit optreden; ga na dat dit bijv. het geval is voor $\cos\alpha = \frac{1}{2}$, d.w.z. $\alpha = \frac{\pi}{3}$.

Is f irreducibel en cos θ een wortel van f, dan is $|\mathbb{Q}(\cos\theta) : \mathbb{Q}| = 3$. Aangezien 3 geen macht is van 2, is de constructie dus niet mogelijk.

III. Constructie van de regelmatige n-hoek.

Dit probleem komt neer op de constructie van $\frac{2\pi}{n}$, dus van $\cos\frac{2\pi}{n}$. $\zeta = e^{\frac{2\pi i}{n}}$ is een primitieve n-de eenheidswortel.
Wegens

$$2\cos\frac{2\pi}{n} = \zeta + \zeta^{-1}$$

is $\mathbb{Q}(\zeta)$ een kwadratische uitbreiding van $\mathbb{Q}(\cos\frac{2\pi}{n})$. Zij G de Galoisgroep van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$; G is een commutatieve groep. Is $\cos\frac{2\pi}{n}$ construeerbaar, dan is $|\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}| = 2^{s-1}$ voor zekere s, dus $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 2^s$. Stel omgekeerd $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 2^s$. Zij H de 2-cyclische ondergroep van G voortgebracht door het automorfisme dat $\zeta \to \zeta^{-1}$. Dan is $\mathbb{Q}(\cos\frac{2\pi}{n}) = \mathrm{Inv}(H)$. Omdat G commutatief is, is H normaaldeler in G. De keten

$$G \supset H \supset (1)$$

is dus te verfijnen tot een compositierij

$$G = G_0 \supset G_1 \supset \dots \supset G_{s-1} = H \supset G_s = (1).$$

Omdat $|G| = 2^s$, is $|G_{i-1}/G_i| = 2$. Er bestaat dus een toren van kwadratische uitbreidingen

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{s-1} = \mathbb{Q}(\cos\frac{2\pi}{n}).$$

Omdat $\mathbb{Q}(\cos\frac{2\pi}{n}) \subseteq \mathbb{R}$, is de constructie in dit geval dus <u>reëel</u> uit te voeren. We hebben dus bewezen :
De regelmatige n-hoek is construeerbaar in het reële affiene vlak dan en slechts dan als $|\mathbb{Q}(\zeta) : \mathbb{Q}| = 2^s$ voor zekere s, $\zeta = e^{\frac{2\pi i}{n}}$.
Nu is $|\mathbb{Q}(\zeta) : \mathbb{Q}| = \mathrm{gr}(\Phi_n) = \varphi(n)$. Stel

$$n = 2^{\nu} p_1^{\nu_1} \dots p_r^{\nu_r},$$

met verschillende oneven priemgetallen $p_1, \dots, p_r$, $\nu_i \geq 1$, $\nu \geq 0$.
Dan is

$$\varphi(n) = 2^{\nu-1}\, p_1^{\nu_1-1} \cdots p_r^{\nu_r-1}(p_1-1)\cdots(p_r-1).$$

$\varphi(n) = 2^s$ kan dus alleen optreden als alle $\nu_i = 1$ en alle p_i-1 een macht van 2 zijn, dus $p_i = 2^{s_i}+1$.
Stel $p = 2^t+1$ is priem. We schrijven

$$t = 2^u t_1,\ t_1 \text{ oneven.}$$

Dan

$$2^t+1 = (2^{2^u}+1)(2^{2^u(t_1-1)} - 2^{2^u(t_1-2)} + \ldots + 1),$$

aangezien voor oneven n

$$x^n+1 = (x+1)(x^{n-1} - x^{n-2} + \ldots + 1).$$

Was dus $t_1 > 1$, dan was 2^t+1 niet priem. Dus moeten de p_i priemgetallen van de gedaante $2^{2^u}+1$ zijn; deze heten <u>priemgetallen van Fermat</u>. Voor $u = 0,1,2,3,4$ vindt men inderdaad priemgetallen $2^{2^u}+1$, n.l.

3, 5, 17, 257, 65537.

Bij $u = 5$ is het mis : $2^{2^5}+1$ is deelbaar door 641.

We hebben dus bewezen :
De regelmatige n-hoek is construeerbaar met passer en lineaal dan en slechts dan als $n = 2^{\nu} p_1 p_2 \cdots p_r$, waarin $p_1, \ldots, p_r$ priemgetallen van de gedaante $2^{2^u}+1$ zijn (priemgetallen van Fermat).

============

Literatuur.

E.Artin , Galois theory. University of Notre Dame, 1948.

——— , Selected topics in modern algebra. Lecture Notes, University of North Carolina, 1954.

G.Birkhoff and S.MacLane , A survey of modern algebra.

N.Bourbaki , Eléments de mathématique. Algèbre, Ch.III : Algèbre multilinéaire, Ch.V : Corps commutatifs. Paris, Hermann.

N.Jacobson , Lectures in abstract algebra.
I : Basis concepts, II : Linear algebra,
III : Theory of fields and Galois theory.
Princeton, Van Nostrand.

S.Lang , Algebra. (Addison - Wesley, 1965).

B.L.van der Waerden , Algebra. (oudere uitgaven : Moderne Algebra). Berlin, Springer Verlag.

H.Weber , Lehrbuch der Algebra I, II.
Braunschweig 1899 , 1912.

===============